ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	2f3679beb84850d1f63c414703a11b20.exe
Full analysis:	https://app.any.run/tasks/edce7179-d437-4c3a-a770-5eaff78739a0
Verdict:	Malicious activity
Threats:	Ave Maria
	Ave Maria malware is a Remote Access Trojan that is also called WARZONE RAT. Hackers use it to control the PCs of their victims remotely and steal information from infected PCs. For example, they can remotely activate the camera to take pictures of a victim and send them to a control server.
Analysis date:	August 22, 2022 at 20:49:04
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojan stealer rat avemaria
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	2F3679BEB84850D1F63C414703A11B20
SHA1:	0A03A19DDA8552EA8CEA1D976EB9126E41409A82
SHA256:	559EC8819D70BD940008D9F57B795F3EC5C68CFB79298579207EB71B840F111F
SSDEEP:	12288:aM1z43a05GVZJiRgl4jcgMW8ayNRxMSt3sq3alpb+ch:FiK0s8Rs7xayNRxMe8Wzp1h

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	off
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2479943
- KB2491683
- KB2506212
- KB2506928
- KB2532531
- KB2533552
- KB2533623
- KB2534111
- KB2545698
- KB2547666
- KB2552343
- KB2560656
- KB2564958
- KB2574819
- KB2579686
- KB2585542
- KB2604115
- KB2620704
- KB2621440
- KB2631813
- KB2639308
- KB2640148
- KB2653956
- KB2654428
- KB2656356
- KB2660075
- KB2667402
- KB2676562
- KB2685811

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)	KB2685813
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2685939
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)	KB2690533
Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972

Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461
Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 83.0 (x86 en-US) (83.0)
Mozilla Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3156016
KB3159398
KB3161102
KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
KB4532945
KB4536952
KB4567409
KB958488
KB976902
KB982018
LocalPack AU Package
LocalPack CA Package
LocalPack GB Package
LocalPack US Package
LocalPack ZA Package
Package 21 for KB2984976
Package 38 for KB2984976
Package 45 for KB2984976
Package 59 for KB2984976
Package 7 for KB2984976
Package 76 for KB2984976
PlatformUpdate Win7 SRV08R2 Package TopLevel
ProfessionalEdition
RDP BlueIP Package TopLevel
RDP WinIP Package TopLevel
RollupFix
UltimateEdition
WUClient SelfUpdate ActiveX
WUClient SelfUpdate Aux TopLevel
WUClient SelfUpdate Core TopLevel
WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS

Drops executable file immediately after starts
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)
cmd.exe (PID: 3804)
DllHost.exe (PID: 2556)

Runs injected code in another process
2f3679beb84850d1f63c414703a11b20.exe (PID: 2204)

Connects to CnC server
2f3679beb84850d1f63c414703a11b20.exe (PID: 2204)

AVEMARIA was detected
2f3679beb84850d1f63c414703a11b20.exe (PID: 2204)

Application was injected by another process
Explorer.EXE (PID: 1068)

Loads dropped or rewritten executable
dism.exe (PID: 3260)

SUSPICIOUS

Reads the computer name
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)
2f3679beb84850d1f63c414703a11b20.exe (PID: 2204)
cmd.exe (PID: 3804)
2f3679beb84850d1f63c414703a11b20.exe (PID: 656)
2f3679beb84850d1f63c414703a11b20.exe (PID: 2812)
powershell.exe (PID: 3500)
2f3679beb84850d1f63c414703a11b20.exe (PID: 2276)

Checks supported languages
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)
2f3679beb84850d1f63c414703a11b20.exe (PID: 2204)
cmd.exe (PID: 3804)
2f3679beb84850d1f63c414703a11b20.exe (PID: 656)
2f3679beb84850d1f63c414703a11b20.exe (PID: 2812)
powershell.exe (PID: 3500)
2f3679beb84850d1f63c414703a11b20.exe (PID: 2276)

Executable content was dropped or overwritten
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)
cmd.exe (PID: 3804)
DllHost.exe (PID: 2556)

Application launched itself
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)
2f3679beb84850d1f63c414703a11b20.exe (PID: 656)

Drops a file with a compile date too recent
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)
cmd.exe (PID: 3804)
DllHost.exe (PID: 2556)

INFO

Reads the computer name
schtasks.exe (PID: 2000)
DllHost.exe (PID: 2556)
dism.exe (PID: 3260)
schtasks.exe (PID: 2448)

Checks supported languages
schtasks.exe (PID: 2000)
dism.exe (PID: 3260)
pkgmgr.exe (PID: 2656)
makecab.exe (PID: 3340)
DllHost.exe (PID: 2556)

Dropped object may contain Bitcoin addresses
2f3679beb84850d1f63c414703a11b20.exe (PID: 3128)

Manual execution by user
2f3679beb84850d1f63c414703a11b20.exe (PID: 2812)

Reads settings of System Certificates
powershell.exe (PID: 3500)

Checks Windows Trust Settings
powershell.exe (PID: 3500)

Creates a directory in Program Files
2f3679beb84850d1f63c414703a11b20.exe (PID: 2204)

Executed via COM
DllHost.exe (PID: 2556)

Static information

TRiD

.exe | Generic CIL Executable (.NET, Mono, etc.) (56.7)
.exe | Win64 Executable (generic) (21.3)
.scr | Windows screen saver (10.1)
.dll | Win32 Dynamic Link Library (generic) (5)
.exe | Win32 Executable (generic) (3.4)

EXIF

EXE

AssemblyVersion:	1.1.0.0
ProductVersion:	1.2.0.0
ProductName:	Morofter
OriginalFileName:	bQzW.exe
LegalTrademarks:	Parts and Pieces
LegalCopyright:	Dinkey Operator ltd
InternalName:	bQzW.exe
FileVersion:	1.2.0.0
FileDescription:	Morofter
CompanyName:	Dinkey Operator
Comments:	
CharacterSet:	Unicode
LanguageCode:	Neutral
FileSubtype:	0
ObjectFileType:	Executable application
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	1.2.0.0
FileVersionNumber:	1.2.0.0
Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0x99fde
UninitializedDataSize:	0
InitializedDataSize:	15360
CodeSize:	622592
LinkerVersion:	48
PEType:	PE32
TimeStamp:	2022:08:22 11:00:22+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	22-Aug-2022 09:00:22
Comments:	
CompanyName:	Dinkey Operator
FileDescription:	Morofter
FileVersion:	1.2.0.0
InternalName:	bQzW.exe
LegalCopyright:	Dinkey Operator ltd
LegalTrademarks:	Parts and Pieces
OriginalFilename:	bQzW.exe
ProductName:	Morofter
ProductVersion:	1.2.0.0
Assembly Version:	1.1.0.0

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	22-Aug-2022 09:00:22
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0

Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000080

Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_EXECUTABLE_IMAGE

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00002000	0x00097FE4	0x00098000	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	7.69879
.rsrc	0x0009A000	0x0000398C	0x00003A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	7.79656
.reloc	0x0009E000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.10191

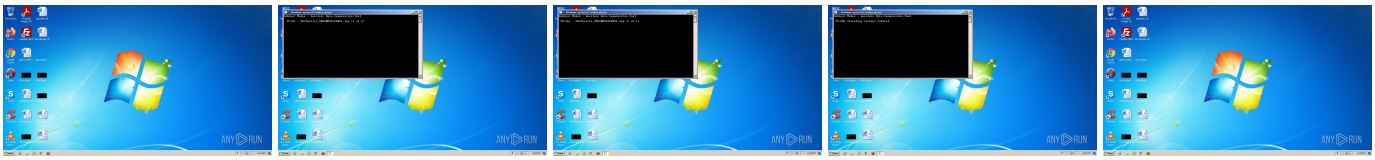
Resources

Title	Entropy	Size	Codepage	Language	Type
1	3.31095	844	UNKNOWN	UNKNOWN	RT_VERSION
32512	1.51664	20	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

mscoree.dll

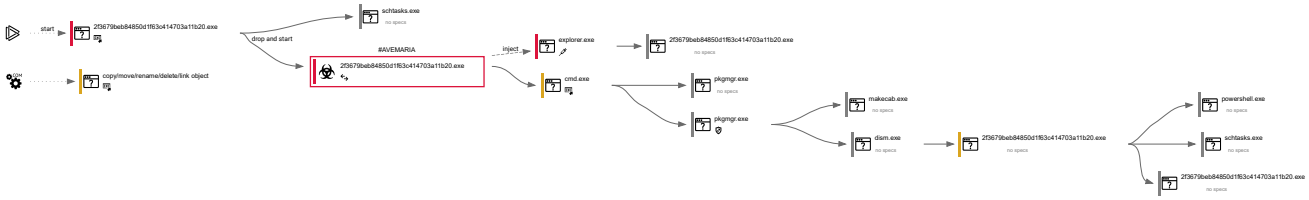
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
55	15	3	3

Behavior graph



Specs description

Program did not start	Low-level access to the HDD	Process was added to the startup	Debug information is available
Probably Tor was used	Behavior similar to spam	Task has injected processes	Executable file was dropped
Known threat	RAM overrun	Network attacks were detected	Integrity level elevation
Connects to the network	CPU overrun	Process starts the services	System was rebooted
Task contains several apps running	Application downloaded the executable file	Actions similar to stealing personal data	Task has apps ended with an error
File is detected by antivirus software	Inspected object has suspicious PE structure	Behavior similar to exploiting the vulnerability	Task contains an error or was rebooted
The process has the malware config			

Process information

PID	CMD	Path	Indicators	Parent process
3128	"C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe"	C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe		Explorer.EXE

Information

User:	admin	**Company:**	Dinkey Operator
Integrity Level:	MEDIUM	**Description:**	Morofter
Exit code:	0	**Version:**	1.2.0.0

2000	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IXiaGIHsOYTxCE" /XML "C:\Users\admin\AppData\Local\Temp\tmpD8EA.tmp"	C:\Windows\System32\schtasks.exe	—	2f3679beb84850d1f63c414703a11b20.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Manages scheduled tasks
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2204	"C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe"	C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe		2f3679beb84850d1f63c414703a11b20.exe

Information

User:	admin	**Company:**	Dinkey Operator
Integrity Level:	MEDIUM	**Description:**	Morofter
Exit code:	0	**Version:**	1.2.0.0

1068	C:\Windows\Explorer.EXE	C:\Windows\Explorer.EXE		—

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Explorer
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

3804	"C:\Windows\System32\cmd.exe"	C:\Windows\System32\cmd.exe		2f3679beb84850d1f63c414703a11b20.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2556	C:\Windows\system32\DllHost.exe /Processid:{3AD05575-8857-4850-9277-11B85BDB8E09}	C:\Windows\system32\DllHost.exe		svchost.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	COM Surrogate
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2784	"C:\Windows\system32\pkgmgr.exe" /n:%temp%\ellocnak.xml	C:\Windows\system32\pkgmgr.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Package Manager
Exit code:	3221226540	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2656	"C:\Windows\system32\pkgmgr.exe" /n:%temp%\ellocnak.xml	C:\Windows\system32\pkgmgr.exe		cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows Package Manager
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3340	"C:\Windows\system32\makecab.exe" C:\Windows\Logs\CBS\CbsPersist_20220822152031.log C:\Windows\Logs\CBS\CbsPersist_20220822152031.cab	C:\Windows\system32\makecab.exe	—	pkgmgr.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Microsoft® Cabinet Maker
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3260	"C:\Windows\system32\dism.exe" /online /norestart /apply-unattend:"C:\Users\admin\AppData\Local\Temp\ellocnak.xml"	C:\Windows\system32\dism.exe	—	pkgmgr.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Dism Image Servicing Utility
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

656	"C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe"	C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe	—	dism.exe

Information

User:	admin	**Company:**	Dinkey Operator
Integrity Level:	HIGH	**Description:**	Morofter
Exit code:	0	**Version:**	1.2.0.0

2812	"C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe"	C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe	—	Explorer.EXE

Information

User:	admin	**Company:**	Dinkey Operator
Integrity Level:	MEDIUM	**Description:**	Morofter
Exit code:	0	**Version:**	1.2.0.0

3500	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\admin\AppData\Roaming\IXiaGIHsOYTxCE.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	2f3679beb84850d1f63c414703a11b20.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows PowerShell
Version:	10.0.14409.1005 (rs1_srvoob.161208-1155)		

2448	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IXiaGIHsOYTxCE" /XML "C:\Users\admin\AppData\Local\Temp\tmpC453.tmp"	C:\Windows\System32\schtasks.exe	—	2f3679beb84850d1f63c414703a11b20.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Manages scheduled tasks
Exit code:	1	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2276	"C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe"	C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe	—	2f3679beb84850d1f63c414703a11b20.exe

Information

User:	admin	**Company:**	Dinkey Operator
Integrity Level:	HIGH	**Description:**	Morofter
Version:	1.2.0.0		

Registry activity

Total events	Read events	Write events	Delete events
5 233	5 175	58	0

Modification events

(PID) Process: (1068) Explorer.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0
Operation: write **Name:** CheckSetting
Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB0100000051CE8C18BA2CDE41B415B910B561518900000000200000000001066000000010000200000000E044973B7C0B28480694817BEC753C4B622BD4F711B24BA56254CFA6D45A2798000000000E80000000020000200000003CD04670BC762EF155E6AD5E65C05B8DED5DC4972EEC660FF982D08D8848AB28300000001DED4469816B52A6E380A73668175BF58C80282E0B6D321347CD88F17CD8E7F0B82C479488664591D2424C2ED493FD0840000000A0F440FADEF5EDE1F3C4E7F66EAE681F23FA51E01D34E3E345B119D72594CD0F32D46B7D6F7502378BC28CB015277E85D2DCE716ED90890AD309695ECF3D9534

(PID) Process: (3128) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3128) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3128) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3128) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2204) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** MaxConnectionsPer1_0Server
Value: 10

(PID) Process: (2204) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** MaxConnectionsPerServer

Value: 10

(PID) Process: (2204) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software_rptls
Operation: write **Name:** Install
Value: C:\Users\admin\AppData\Local\Temp\2f3679beb84850d1f63c414703a11b20.exe

(PID) Process: (3804) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3804) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3804) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3804) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1068) Explorer.EXE **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (656) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (656) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (656) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (656) 2f3679beb84850d1f63c414703a11b20.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3500) powershell.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3500) powershell.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3500) powershell.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3500) powershell.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3500) powershell.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

Files activity

Executable files	Suspicious files	Text files	Unknown types
3	6	4	0

Dropped files

PID	Process	Filename	Type
2656	pkgmgr.exe	C:\Windows\Logs\CBS\CbsPersist_20220822152031.log	–

		MD5: —	SHA256: —	
3128	2f3679beb84850d1f63c414703a11b20.exe	C:\Users\admin\AppData\Local\Temp\tmpD8EA.tmp		xml
		MD5: 859EC1107C8F4B632459FDEBE8AEBA19	SHA256: B667C324908CB5E004B4B0F4780DC90AA8EEDA3DAA4A16D5D5E67ED47EE72FEF	
3804	cmd.exe	C:\Users\admin\AppData\Local\Temp\ellocnak.xml		xml
		MD5: 427EB7374887305B72F5C552837C9036	SHA256: B3F421780A49CBE680A317259D4DF9CE1D0CDACA3020B4DF0DC18CC01D68CCBB	
3128	2f3679beb84850d1f63c414703a11b20.exe	C:\Users\admin\AppData\Roaming\lXiaGIHsOYTxCE.exe		executable
		MD5: 2F3679BEB84850D1F63C414703A11B20	SHA256: 559EC8819D70BD940008D9F57B795F3EC5C68CFB79298579207EB71B840F111F	
3804	cmd.exe	C:\Users\admin\AppData\Local\Temp\dismcore.dll		executable
		MD5: 6B906764A35508A7FD266CDD512E46B1	SHA256: FC0C90044B94B080F307C16494369A0796AC1D4E74E7912BA79C15CCA241801C	
3340	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_3340_4		binary
		MD5: A439AD6D04C099EC6F85B3B5B96A3AC3	SHA256: 8C08BEA3C051DB4252EB452FFF7F03A843EE5B83177C488A59308F3AF1789521	
3340	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_3340_2		binary
		MD5: F7BB56E52701D76FCE4941B41C44DB3F	SHA256: A35F5A8709EC880025656ADA2F4AFE1EC6207C4FAE69CD654632016F61A9AFFD	
3340	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_3340_3		binary
		MD5: 90086448F6F50602D5C907525626B64F	SHA256: 14E45D73B56F16A49A73ED44DFE1C4889CC8457911A43146735CF5930E3A5F81	
2556	DllHost.exe	C:\Windows\System32\dismcore.dll		executable
		MD5: 6B906764A35508A7FD266CDD512E46B1	SHA256: FC0C90044B94B080F307C16494369A0796AC1D4E74E7912BA79C15CCA241801C	
3340	makecab.exe	C:\Windows\Logs\CBS\CbsPersist_20220822152031.cab		compressed
		MD5: A8D25FDC0CC9C0CC1510B0041B7C6838	SHA256: 9995DFCB82C276DC5E8120BA116613393ED2D555F29B14EC79C6155A6075B9EF	
2656	pkgmgr.exe	C:\Windows\Logs\CBS\CBS.log		text
		MD5: A6300AA852E65F765F516613B56FF278	SHA256: 1A65DAF9C631C38B200E7943D70204CCC4ECF1FF5CB3622C2BE1AF41FF0714C1	
3340	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_3340_6		binary
		MD5: C8E1DBBCFC190FDB17E199068E9ACC8D	SHA256: 4CA90AC9A4C923B77E3A23F57D87EF5EC83820868F22BC9BC0A587107E0705EB	
656	2f3679beb84850d1f63c414703a11b20.exe	C:\Users\admin\AppData\Local\Temp\tmpC453.tmp		xml
		MD5: 859EC1107C8F4B632459FDEBE8AEBA19	SHA256: B667C324908CB5E004B4B0F4780DC90AA8EEDA3DAA4A16D5D5E67ED47EE72FEF	
3340	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_3340_5		binary
		MD5: 90086448F6F50602D5C907525626B64F	SHA256: 14E45D73B56F16A49A73ED44DFE1C4889CC8457911A43146735CF5930E3A5F81	
3500	powershell.exe	C:\Users\admin\AppData\Local\Temp\lyxnkgv0.psz.ps1		—
		MD5: —	SHA256: —	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	1	0	1

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2204	2f3679beb84850d1f63c414703a11b20.exe	76.8.53.133:1198	—	Quonix Networks Inc.	US	malicious

DNS requests

No data

Threats

Found threats are available for the paid subscriptions

Debug output strings

No debug info