



## General Info

File name:	Remittance Advice.exe
Full analysis:	<a href="https://app.any.run/tasks/cbe1aa6a-5176-420f-8656-71d3cf469a33">https://app.any.run/tasks/cbe1aa6a-5176-420f-8656-71d3cf469a33</a>
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 19:17:33
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojanratstealeravemariaarkeiwarzone
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	DCEA2976EA8E3FCC636AE0D4C1FEDB05
SHA1:	0F04F8E5ABFD95105146FDDDB1104B8B754D9600
SHA256:	1D84CE7E67665AA6F9B94DC7BEE30E326C647B8819BF7B155A68F6F2CE54FC60
SSDEEP:	12288:VqllfpEHsgDag6n04imn/cjEsVXTVgsaQ2DmbaZQWx18Ui6JccGlrj:IfCA04i+oNVjVgJg9C8Ui6Jcgr

### 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)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)	KB3161949
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)	KB3170735
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)	KB3172605
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)	KB3179573
Mozilla Firefox 83.0 (x86 en-US) (83.0)	KB3184143
Mozilla Maintenance Service (83.0.0.7621)	KB3185319
Notepad++ (32-bit x86) (7.9.1)	KB4019990
Opera 12.15 (12.15.1748)	KB4040980
QGA (2.14.33)	KB4474419
Skype version 8.29 (8.29)	KB4490628
VLC media player (3.0.11)	KB4524752
WinRAR 5.91 (32-bit) (5.91.0)	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	SUSPICIOUS	INFO
<p><b>Drops executable file immediately after starts</b></p> <p>Remittance Advice.exe (PID: 3496)</p> <p>cmd.exe (PID: 1896)</p> <p>DllHost.exe (PID: 3384)</p>	<p><b>Reads the computer name</b></p> <p>Remittance Advice.exe (PID: 3496)</p> <p>Remittance Advice.exe (PID: 2824)</p> <p>cmd.exe (PID: 1896)</p> <p>Remittance Advice.exe (PID: 1012)</p> <p>Remittance Advice.exe (PID: 3236)</p> <p>powershell.exe (PID: 2844)</p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p> <p>Remittance Advice.exe (PID: 976)</p>	<p><b>Reads the computer name</b></p> <p>schtasks.exe (PID: 2520)</p> <p>dism.exe (PID: 3020)</p> <p>DllHost.exe (PID: 3384)</p> <p>schtasks.exe (PID: 2252)</p> <p>schtasks.exe (PID: 3336)</p>
<p><b>Runs injected code in another process</b></p> <p>Remittance Advice.exe (PID: 2824)</p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p>	<p><b>Executable content was dropped or overwritten</b></p> <p>Remittance Advice.exe (PID: 3496)</p> <p>cmd.exe (PID: 1896)</p> <p>DllHost.exe (PID: 3384)</p>	<p><b>Checks supported languages</b></p> <p>schtasks.exe (PID: 2520)</p> <p>pkgmgr.exe (PID: 2936)</p> <p>DllHost.exe (PID: 3384)</p> <p>makecab.exe (PID: 2868)</p> <p>dism.exe (PID: 3020)</p> <p>schtasks.exe (PID: 2252)</p> <p>schtasks.exe (PID: 3336)</p>
<p><b>Application was injected by another process</b></p> <p>Explorer.EXE (PID: 1348)</p>	<p><b>Checks supported languages</b></p> <p>Remittance Advice.exe (PID: 3496)</p> <p>cmd.exe (PID: 1896)</p> <p>Remittance Advice.exe (PID: 2824)</p> <p>Remittance Advice.exe (PID: 1012)</p> <p>Remittance Advice.exe (PID: 3236)</p> <p>powershell.exe (PID: 2844)</p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p> <p>Remittance Advice.exe (PID: 976)</p>	<p><b>Manual execution by user</b></p> <p>Remittance Advice.exe (PID: 3236)</p> <p>Remittance Advice.exe (PID: 976)</p>
<p><b>AVEMARIA was detected</b></p> <p>Remittance Advice.exe (PID: 2824)</p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p>	<p><b>Drops a file with a compile date too recent</b></p> <p>Remittance Advice.exe (PID: 3496)</p> <p>cmd.exe (PID: 1896)</p> <p>DllHost.exe (PID: 3384)</p>	<p><b>Checks Windows Trust Settings</b></p> <p>powershell.exe (PID: 2844)</p>
<p><b>Connects to CnC server</b></p> <p>Remittance Advice.exe (PID: 2824)</p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p>		<p><b>Reads settings of System Certificates</b></p> <p>powershell.exe (PID: 2844)</p>
<p><b>ARKEI detected by memory dumps</b></p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p>		
<p><b>WARZONE detected by memory dumps</b></p> <p>Remittance Advice.exe (PID: 1868)</p> <p>Remittance Advice.exe (PID: 1796)</p>		

Creates a directory in Program Files

Remittance Advice.exe (PID: 2824)

Remittance Advice.exe (PID: 1868)

Application launched itself

Remittance Advice.exe (PID: 3496)

Remittance Advice.exe (PID: 1012)

Remittance Advice.exe (PID: 3236)

Executed via COM

DllHost.exe (PID: 3384)

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

MachineType: Intel 386 or later, and compatibles

TimeStamp: 2022:08:19 16:49:13+02:00

PEType: PE32

LinkerVersion: 48

CodeSize: 726016

InitializedDataSize: 1536

UninitializedDataSize: 0

EntryPoint: 0xb321e

OSVersion: 4

ImageVersion: 0

SubsystemVersion: 4

Subsystem: Windows GUI

FileVersionNumber: 1.0.0.0

ProductVersionNumber: 1.0.0.0

FileFlagsMask: 0x003f

FileFlags: (none)

FileOS: Win32

ObjectFileType: Executable application

FileSubtype: 0

LanguageCode: Neutral

CharacterSet: Unicode

Comments:

CompanyName: Microsoft Corporation

FileDescription: Snakii

FileVersion: 1.0.0.0

InternalName: BbwwPt.exe

LegalCopyright: Copyright © 2017

LegalTrademarks:

OriginalFileName: BbwwPt.exe

ProductName: Snakii

ProductVersion: 1.0.0.0

AssemblyVersion: 1.0.0.0

Summary

Architecture: IMAGE\_FILE\_MACHINE\_I386

Subsystem: IMAGE\_SUBSYSTEM\_WINDOWS\_GUI

Compilation Date: 19-Aug-2022 14:49:13

Comments:

CompanyName: Microsoft Corporation

FileDescription: Snakii

FileVersion: 1.0.0.0

InternalName: BbwwPt.exe

LegalCopyright: Copyright © 2017

LegalTrademarks:

OriginalFilename: BbwwPt.exe

ProductName: Snakii

ProductVersion: 1.0.0.0

Assembly Version: 1.0.0.0

DOS Header

Magic number: MZ

Bytes on last page of file: 0x0090

Pages in file: 0x0003

PE Headers

Signature: PE

Machine: IMAGE\_FILE\_MACHINE\_I386

Number of sections: 3

Relocations:	0x0000	Time date stamp:	19-Aug-2022 14:49:13
Size of header:	0x0004	Pointer to Symbol Table:	0x00000000
Min extra paragraphs:	0x0000	Number of symbols:	0
Max extra paragraphs:	0xFFFF	Size of Optional Header:	0x00E0
Initial SS value:	0x0000	Characteristics:	IMAGE_FILE_32BIT_MACHINE
Initial SP value:	0x00B8		IMAGE_FILE_EXECUTABLE_IMAGE
Checksum:	0x0000		
Initial IP value:	0x0000		
Initial CS value:	0x0000		
Overlay number:	0x0000		
OEM identifier:	0x0000		
OEM information:	0x0000		
Address of NE header:	0x00000080		

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00002000	0x000B1224	0x000B1400	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	7.64514
.src	0x000B4000	0x00000390	0x00000400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	2.89065
.reloc	0x000B6000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.10191

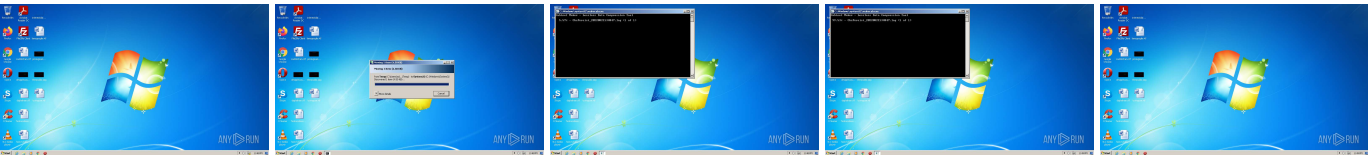
Resources

Title	Entropy	Size	Codepage	Language	Type
1	3.28932	820	UNKNOWN	UNKNOWN	RT_VERSION

Imports

mscoree.dll
-------------

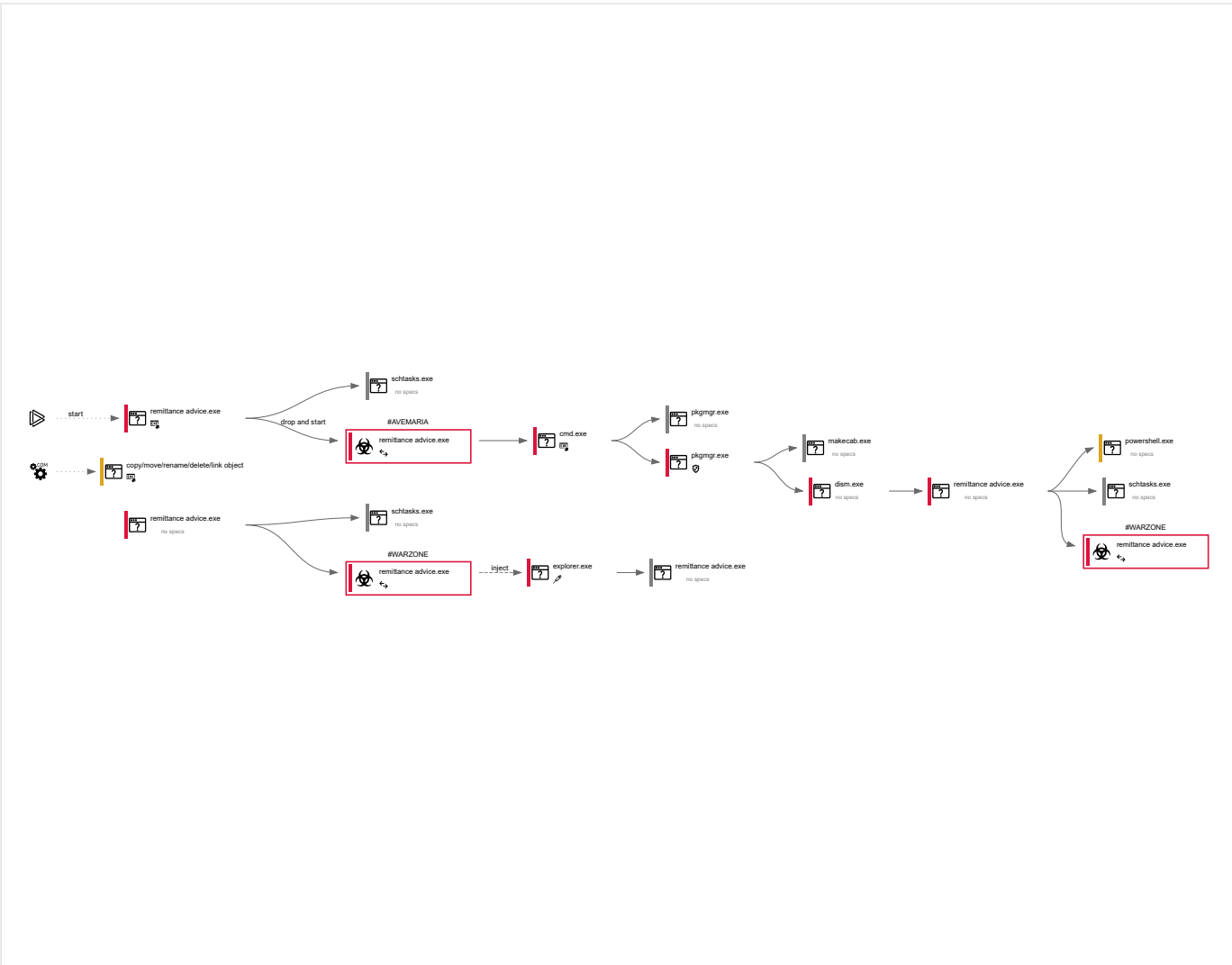
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
66	18	10	2

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
3496	"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"	C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe		Explorer.EXE
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Snakii	
Exit code:	0	Version:	1.0.0.0	

2520	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NJRYyempQ" /XML "C:\Users\admin\AppData\Local\Temp\tmp4E4A.tmp"	C:\Windows\System32\schtasks.exe	—	Remittance Advice.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">Manages scheduled tasks</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">6.1.7600.16385 (win7_rtm.090713-1255)</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	MEDIUM	Description:	Manages scheduled tasks		Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks																
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)																
2824	"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"	C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe		Remittance Advice.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">Snakii</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">1.0.0.0</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	MEDIUM	Description:	Snakii		Exit code:	0	Version:	1.0.0.0	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	MEDIUM	Description:	Snakii																
Exit code:	0	Version:	1.0.0.0																
1896	"C:\Windows\System32\cmd.exe"	C:\Windows\System32\cmd.exe		Remittance Advice.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">Windows Command Processor</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">6.1.7601.17514 (win7sp1_rtm.101119-1850)</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	MEDIUM	Description:	Windows Command Processor		Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	MEDIUM	Description:	Windows Command Processor																
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)																
3384	C:\Windows\system32\DllHost.exe /Processid:{3AD05575-8857-4850-9277-11B85BDB8E09}	C:\Windows\system32\DllHost.exe		svchost.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>HIGH</td><td>Description:</td><td colspan="2">COM Surrogate</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">6.1.7600.16385 (win7_rtm.090713-1255)</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	HIGH	Description:	COM Surrogate		Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	HIGH	Description:	COM Surrogate																
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)																
2372	"C:\Windows\system32\pkgmgr.exe" /n:%temp%\ellocnak.xml	C:\Windows\system32\pkgmgr.exe	—	cmd.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">Windows Package Manager</td></tr><tr><td>Exit code:</td><td>3221226540</td><td>Version:</td><td colspan="2">6.1.7601.17514 (win7sp1_rtm.101119-1850)</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	MEDIUM	Description:	Windows Package Manager		Exit code:	3221226540	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	MEDIUM	Description:	Windows Package Manager																
Exit code:	3221226540	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)																
2936	"C:\Windows\system32\pkgmgr.exe" /n:%temp%\ellocnak.xml	C:\Windows\system32\pkgmgr.exe		cmd.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>HIGH</td><td>Description:</td><td colspan="2">Windows Package Manager</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">6.1.7601.17514 (win7sp1_rtm.101119-1850)</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	HIGH	Description:	Windows Package Manager		Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	HIGH	Description:	Windows Package Manager																
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)																
2868	"C:\Windows\system32\makecab.exe" C:\Windows\Logs\CBS\CbsPersist_20220822134847.log C:\Windows\Logs\CBS\CbsPersist_20220822134847.cab	C:\Windows\system32\makecab.exe	—	pkgmgr.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>HIGH</td><td>Description:</td><td colspan="2">Microsoft® Cabinet Maker</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">6.1.7600.16385 (win7_rtm.090713-1255)</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	HIGH	Description:	Microsoft® Cabinet Maker		Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	HIGH	Description:	Microsoft® Cabinet Maker																
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)																
3020	"C:\Windows\system32\dism.exe" /online /norestart /apply-unattend:"C:\Users\admin\AppData\Local\Temp\ellocnak.xml"	C:\Windows\system32\dism.exe	—	pkgmgr.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>HIGH</td><td>Description:</td><td colspan="2">Dism Image Servicing Utility</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">6.1.7600.16385 (win7_rtm.090713-1255)</td></tr></table>					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)	
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)																
1012	"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"	C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe	—	dism.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>HIGH</td><td>Description:</td><td colspan="2">Snakii</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">1.0.0.0</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	HIGH	Description:	Snakii		Exit code:	0	Version:	1.0.0.0	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	HIGH	Description:	Snakii																
Exit code:	0	Version:	1.0.0.0																
3236	"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"	C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe	—	Explorer.EXE															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">Snakii</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">1.0.0.0</td></tr></table>					User:	admin	Company:	Microsoft Corporation		Integrity Level:	MEDIUM	Description:	Snakii		Exit code:	0	Version:	1.0.0.0	
User:	admin	Company:	Microsoft Corporation																
Integrity Level:	MEDIUM	Description:	Snakii																
Exit code:	0	Version:	1.0.0.0																
2844	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	Remittance Advice.exe															



Add-MpPreference -ExclusionPath "C:\Users\admin\AppData\Roaming\NJRyefmpQ.exe"

Information

User:adminCompany:Microsoft Corporation

Integrity Level:HIGHDescription:Windows PowerShell

Exit code:1Version:10.0.14409.1005 (rs1\_srvoob.161208-1155)

2252

"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NJRyefmpQ" /XML "C:\Users\admin\AppData\Local\Temp\tmp1003.tmp"

C:\Windows\System32\schtasks.exe

—

Remittance Advice.exe

Information

User:adminCompany:Microsoft Corporation


Integrity Level:HIGHDescription:Manages scheduled tasks

Exit code:1Version:6.1.7600.16385 (win7\_rtm.090713-1255)

1868

"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"

C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe



Remittance Advice.exe

Information

User:adminCompany:Microsoft Corporation

Integrity Level:HIGHDescription:Snakii

Version:1.0.0.0

3336

"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NJRyefmpQ" /XML "C:\Users\admin\AppData\Local\Temp\tmp33C8.tmp"

C:\Windows\System32\schtasks.exe

—

Remittance Advice.exe

Information

User:adminCompany:Microsoft Corporation


Integrity Level:MEDIUMDescription:Manages scheduled tasks

Exit code:1Version:6.1.7600.16385 (win7\_rtm.090713-1255)

1796

"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"

C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe



Remittance Advice.exe

Information

User:adminCompany:Microsoft Corporation


Integrity Level:MEDIUMDescription:Snakii

Version:1.0.0.0

1348

C:\Windows\Explorer.EXE

C:\Windows\Explorer.EXE



—

Information

User:adminCompany:Microsoft Corporation

Integrity Level:MEDIUMDescription:Windows Explorer

Version:6.1.7600.16385 (win7\_rtm.090713-1255)

976

"C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe"

C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe

—

Explorer.EXE

Information

User:adminCompany:Microsoft Corporation

Integrity Level:MEDIUMDescription:Snakii

Version:1.0.0.0

## Registry activity

Total events	Read events	Write events	Delete events
6 199	6 076	123	0

## Modification events

(PID) Process:	(1348) Explorer.EXE	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	LanguageList
Value:	en-US		
(PID) Process:	(3496) Remittance Advice.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		
(PID) Process:	(3496) Remittance Advice.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		
(PID) Process:	(3496) Remittance Advice.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write	Name: UNCAsIntranet
Value: 1	
(PID) Process: (3496) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: AutoDetect
Value: 0	
(PID) Process: (2824) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write	Name: MaxConnectionsPer1_0Server
Value: 10	
(PID) Process: (2824) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write	Name: MaxConnectionsPerServer
Value: 10	
(PID) Process: (2824) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\_rptls
Operation: write	Name: Install
Value: C:\Users\admin\AppData\Local\Temp\Remittance Advice.exe	
(PID) Process: (1896) cmd.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: ProxyBypass
Value: 1	
(PID) Process: (1896) cmd.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: IntranetName
Value: 1	
(PID) Process: (1896) cmd.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: UNCAsIntranet
Value: 1	
(PID) Process: (1896) cmd.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: AutoDetect
Value: 0	
(PID) Process: (1012) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: ProxyBypass
Value: 1	
(PID) Process: (1012) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: IntranetName
Value: 1	
(PID) Process: (1012) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: UNCAsIntranet
Value: 1	
(PID) Process: (1012) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: AutoDetect
Value: 0	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write	Name: MaxConnectionsPer1_0Server
Value: 10	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write	Name: MaxConnectionsPerServer
Value: 10	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: ProxyBypass
Value: 1	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: IntranetName
Value: 1	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: UNCAsIntranet
Value: 1	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write	Name: AutoDetect
Value: 0	
(PID) Process: (1868) Remittance Advice.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write	Name: ProxyEnable
Value: 0	

[https://any.run/report/1d84ce7e67665aa6f9b94dc7bee30e326c647b8819bf7b155a68f6f2ce54fc60/cbe1aa6a-5176-420f-8656-71d3cf469a33?\\_...](https://any.run/report/1d84ce7e67665aa6f9b94dc7bee30e326c647b8819bf7b155a68f6f2ce54fc60/cbe1aa6a-5176-420f-8656-71d3cf469a33?_...) 11/14

<b>Value:</b> 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000FDEED3ACA194C41A6F4BE7809985ACD0000000020000000001066000000100002000000084313803BBE24081A80C6E553481B9C27B948ED7EC870EC7D91FB703FA91D94300000000E8000000002000200000003FF47FF19E81046241115B4A63A6207E994537FADD233911CEC22FCD8394E00C00000002F4D6ED5D1ACB96B917993BF7A315488A4CB5253DBEE50826B308666A48B35FDBBD30442483573E39BCA8935AEC9016B30D663988229DAD746AFB4C3708BFEE5407AF0B59EC146F90333E85885AA8B1AC86D565E89B68C7243299E2F0CBB9A3FCAC569BB4587F15F49838FB2D6FBCC7227B19FC19ADDCC9412A44AA16723CA716549AC3B5D000E2295CBBEC86FE8E94252C4511479D14148BBE29E06273D21BC757C0D6A32D9FA75608465F1CB668B524250C4F2BF80AFD8CD5FF236D02327B40000000C22FCD51F43959345402BD60AC64F368C0AFAA45FFB27545B1B3BFA2753BD6C725D8E64B3DC753D39949320DF66CD74A0799D3CC219468E8DF86258F8CDDE31			
<b>(PID) Process:</b>	(1348) Explorer.EXE	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{E8433B72-5842-4d43-8645-BC2C35960837}.check.100
<b>Operation:</b>	write	<b>Name:</b>	CheckSetting
<b>Value:</b> 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000FDEED3ACA194C41A6F4BE7809985ACD000000002000000000010660000001000020000000EE59DC54774A5125A7611DE5CA95857A7398314BF746E89C0B211DDFD5BE67A600000000E8000000002000020000000AAD6EC777FD3F770AEF7F953ACEAE44F7BB511530B6370B1AD2D17F72B6C0E41C000000014B0F30FB0EDE432707BC3580B4691603240EB5F11A540D7C39102039CF0946B845757F1A8152D522CF3C727BD8717B77F3342E6ED37FDCF232F500A951B0325DE0F659F956BB91DF99F2FF168AC44AF6D664805ADE49AF5444B2F8A7E9C3A9EDDA3A6417CE826B1631479B4B01EE929FEF5344AFD51E65CD1A1066B6C9D3778BB193FFDFF8A6D0D7FF2CA132A5C52E7B317A9703580AFE3F9D1A133BD56200DF985048ACE4775C83E181E958DBFCA3B3EEDCED8BCCD93C406FF4E1751E032240000000A552EEA0D8280428A5116BFBC2DDCC94BD9416E65CA881A09ECCF55F7E123404274EBE39BDC981C705542C5757DDE8FA052E960AFB17DA8610B76FD64C4C8A62			
<b>(PID) Process:</b>	(1348) Explorer.EXE	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{E8433B72-5842-4d43-8645-BC2C35960837}.check.102
<b>Operation:</b>	write	<b>Name:</b>	CheckSetting
<b>Value:</b> 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000FDEED3ACA194C41A6F4BE7809985ACD000000002000000000010660000001000020000000DBAEABCF80530001FFF5FCDA A9E080E356C240148120DC035F89B0B6333FA22700000000E800000000200020000000D1ED31E29D055B10345C08BE3DD44A49D2BA2DB2ACED97D7CA7C15DFF45679C0000000CE147DE386AC50416D6843481B7C16A051C5BB3384A14C467991719C6B3E20FCE562B1CFC6F556488877FCF3B061FF1BCFF0388F27F5099E30BB7049D473616E392DDA23B4B6CECFD3CA07B5E3FE075103B64D5355E85A2CF3E18D705EA59BED363EC97CE707CD5677F8AD9E388AE52D5174E5839A02E121EE5BE0D23E1C1443B6EB2091723BEB7A9B80E0241FC86EEE9114B6E3759E87EDA2BB1FC08D30493FAEB58531517C227B6E728C5236EBFE7C9C9A14A1AA36C50D25B6BC4F47801A524000000F5ED8097A03A1DE576BCD73BF5D0FA2FFB9426311F4D67FBC0B3EBA79B6F359E0B92ABE413531D7178A9B6BFBA3A62FBC369F77346F4BA4496894D70CC8B6C4			
<b>(PID) Process:</b>	(1348) Explorer.EXE	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100
<b>Operation:</b>	write	<b>Name:</b>	CheckSetting
<b>Value:</b> 23004100430042006C006F0062000000000000000000000100000000000000000000			
<b>(PID) Process:</b>	(1348) Explorer.EXE	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101
<b>Operation:</b>	write	<b>Name:</b>	CheckSetting
<b>Value:</b> 23004100430042006C006F0062000000000000000000000100000000000000000000			
<b>(PID) Process:</b>	(1348) Explorer.EXE	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
<b>Operation:</b>	write	<b>Name:</b>	CheckSetting
<b>Value:</b> 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000FDEED3ACA194C41A6F4BE7809985ACD000000002000000000010660000001000020000000E5F735C9E2CD006266B837CFB C3FD39BEBF5C8D0EDF14A64D7810BB6B685722200000000E80000000020002000000095CEBFC0CCEC76F004939502446B71B2742FDDEFA796A77DB6B1F42B6B85CE68000000007415396C71BB4693FE919FEF8678A0AC15526F6E82D1BE5B206BE1944AA43D2BA23352873DD867F5E94FB48E69221EF311CE9FEA8F8D38F05A3731051C9CFDA9650A500DA232C3DDBB5933F935C551719848B25990D28ADA4833E54C040B02F0762350E96321F43EAA684BDF113D63A74B539A2786E96D1AA4E71DE04E129C4DFFDF7B11858ABF32664D197EC158A8763C09C4C8E23492A0345CED806ACDF957BDBD67422E8B3FF87F217A47840000000551D5F4AD0A437AC40321FD96B2B8E2F7C2D7F0DB067E066CB50EDB1EFBA8B9434EBF6D3F00D35D3D48A66D8ECD62F383587FC0C7E94CCDF9C666A2B8ACC722D			
<b>(PID) Process:</b>	(1348) Explorer.EXE	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0
<b>Operation:</b>	write	<b>Name:</b>	CheckSetting
<b>Value:</b> 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000FDEED3ACA194C41A6F4BE7809985ACD000000002000000000010660000001000020000000399BF9815D482E6D49838F1CB6046D8132237E0E24DD0D29E0F5EAB7D92D2D9F00000000E8000000002000200000007CA99180C7299FBE3C5D154512CD695B4191DC4F792D47DEFB300DF8967DB630000000ED2FB E0477EE5E4890014373D4A8B6A5F29F3F6A1337EF9C79692C3D9820538EB985446387B9E629F188D7EC8D2C835D4000000075647D269435776F48AEA75F5FDE2355A795A093A41A72BFE E77A9150260C56C01CBFA28AEC7E34B0F14293538582D8D3013E98C871F86D7ED728697A038571			
<b>(PID) Process:</b>	(3236) Remittance Advice.exe	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
<b>Operation:</b>	write	<b>Name:</b>	ProxyBypass
<b>Value:</b> 1			
<b>(PID) Process:</b>	(3236) Remittance Advice.exe	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
<b>Operation:</b>	write	<b>Name:</b>	IntranetName
<b>Value:</b> 1			
<b>(PID) Process:</b>	(3236) Remittance Advice.exe	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
<b>Operation:</b>	write	<b>Name:</b>	UNCAsIntranet
<b>Value:</b> 1			
<b>(PID) Process:</b>	(3236) Remittance Advice.exe	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
<b>Operation:</b>	write	<b>Name:</b>	AutoDetect
<b>Value:</b> 0			
<b>(PID) Process:</b>	(1796) Remittance Advice.exe	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
<b>Operation:</b>	write	<b>Name:</b>	MaxConnectionsPer1_0Server
<b>Value:</b> 10			
<b>(PID) Process:</b>	(1796) Remittance Advice.exe	<b>Key:</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
<b>Operation:</b>	write	<b>Name:</b>	MaxConnectionsPerServer
<b>Value:</b> 10			

## Files activity

Executable files	Suspicious files	Text files	Unknown types
3	8	5	1

### Dropped files

PID	Process	Filename	Type
2936	pgkmgr.exe	C:\Windows\Logs\CBS\CbsPersist_20220822134847.log MD5: — SHA256: —	—
2936	pgkmgr.exe	C:\Windows\Logs\CBS\CBS.log MD5: F6C09606800E5A1745ACE67B688BE82D SHA256: C65684301196062A35632D631DDE3FF689C51AD642B73B43C4ADA1D05DB60E5D	text
3496	Remittance Advice.exe	C:\Users\admin\AppData\Local\Temp\tmp4E4A.tmp MD5: BDD2DE1FF621F71378242BFDA9792CA SHA256: E9D720538F13B8B6E6A27A9DBD19AAD6CAEB434BDA9F95920391F03CC5C3C757	xml
1896	cmd.exe	C:\Users\admin\AppData\Local\Temp\ellocnak.xml MD5: 427EB7374887305B72F5C552837C9036 SHA256: B3F421780A49CBE680A317259D4DF9CE1D0CDACA3020B4DF0DC18CC01D68CCBB	xml
1896	cmd.exe	C:\Users\admin\AppData\Local\Temp\dismcore.dll MD5: 6B906764A35508A7FD266CDD512E46B1 SHA256: FC0C90044B94B080F307C16494369A0796AC1D4E74E7912BA79C15CCA241801C	executable
2868	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_2868_3 MD5: 035ED6C3CF4980882D7A7DE2F7703282 SHA256: 8DC63DB6CC040BE8DB0178EC376FB152074C27FE89E3344283C08DE24C12FAA4	binary
3384	DllHost.exe	C:\Windows\System32\dismcore.dll MD5: 6B906764A35508A7FD266CDD512E46B1 SHA256: FC0C90044B94B080F307C16494369A0796AC1D4E74E7912BA79C15CCA241801C	executable
2868	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_2868_4 MD5: A439AD6D04C099EC6F85B3B5B96A3AC3 SHA256: 8C08BEA3C051DB4252EB452FFF7F03A843EE5B83177C488A59308F3AF1789521	binary
2868	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_2868_2 MD5: F7BB56E52701D76FCE4941B41C44DB3F SHA256: A35F5A8709EC880025656ADA2FAFE1EC6207C4FAE69CD654632016F61A9AFFD	binary
3496	Remittance Advice.exe	C:\Users\admin\AppData\Roaming\NJRYefmpQ.exe MD5: DCEA2976EA8E3FCC636AE0D4C1FEDB05 SHA256: 1D84CE7E67665AA6F9B94DC7BEE30E326C647B8819BF7B155A68F6F2CE54FC60	executable
2868	makecab.exe	C:\Windows\Logs\CBS\CbsPersist_20220822134847.cab MD5: F3FE436C28E40F8091B8AAC68DB67D88 SHA256: A773665CAC3F89EC1C56364349A8F723F9EDCA8EABA19672B299AD57063EF02C	compressed
1012	Remittance Advice.exe	C:\Users\admin\AppData\Local\Temp\tmp1003.tmp MD5: BDD2DE1FF621F71378242BFDA9792CA SHA256: E9D720538F13B8B6E6A27A9DBD19AAD6CAEB434BDA9F95920391F03CC5C3C757	xml
2868	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_2868_6 MD5: C8E1DBBCFC190FDB17E199068E9ACC8D SHA256: 4CA90AC9A4C923B77E3A23F57D87EF5EC83820868F22BC9BC0A587107E0705EB	binary
2868	makecab.exe	C:\Users\admin\AppData\Local\Temp\cab_2868_5 MD5: 035ED6C3CF4980882D7A7DE2F7703282 SHA256: 8DC63DB6CC040BE8DB0178EC376FB152074C27FE89E3344283C08DE24C12FAA4	binary
2844	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive MD5: 446DD1CF97EABA21CF14D03AEB79F27 SHA256: A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF	dbf
2844	powershell.exe	C:\Users\admin\AppData\Local\Temp\ic4nygoe.21s.psm1 MD5: C4CA4238A0B923820DCC509A6F75849B SHA256: 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2844	powershell.exe	C:\Users\admin\AppData\Local\Temp\li3awqpm.sc1.ps1 MD5: C4CA4238A0B923820DCC509A6F75849B SHA256: 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3236	Remittance Advice.exe	C:\Users\admin\AppData\Local\Temp\tmp33C8.tmp MD5: BDD2DE1FF621F71378242BFDA9792CA SHA256: E9D720538F13B8B6E6A27A9DBD19AAD6CAEB434BDA9F95920391F03CC5C3C757	xml

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
2	8	2	7

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1656	sipnotify.exe	HEAD	200	23.205.225.13:80	http://query.prod.cms.rt.microsoft.com/cms/api/am/binary/R2JgkA?v=132924875993280000	NL	—	—	whitelisted
1868	Remittance Advice.exe	GET	—	5.206.225.104:80	http://5.206.225.104/dll/upnp.exe	NL	—	—	suspicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
—	—	51.124.78.146:443	—	Microsoft Corporation	GB	whitelisted
1656	sipnotify.exe	23.205.225.13:80	query.prod.cms.rt.microsoft.com	GTT Communications Inc.	NL	unknown
2824	Remittance Advice.exe	37.120.206.69:5200	—	Secure Data Systems SRL	RO	

						malicious
1352	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	—	US	whitelisted
1868	Remittance Advice.exe	37.120.206.69:5200	—	Secure Data Systems SRL	RO	malicious
1868	Remittance Advice.exe	5.206.225.104:80	—	Dotsi, Unipessoal Lda.	NL	suspicious
1796	Remittance Advice.exe	37.120.206.69:5200	—	Secure Data Systems SRL	RO	malicious

DNS requests

Domain	IP	Reputation
query.prod.cms.rt.microsoft.com	23.205.225.13	whitelisted
settings-win.data.microsoft.com	20.73.194.208	whitelisted

Threats

PID	Process	Class	Message
2824	Remittance Advice.exe	A Network Trojan was detected	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)
2824	Remittance Advice.exe	A Network Trojan was detected	AV TROJAN Ave Maria RAT CnC Response
2824	Remittance Advice.exe	A Network Trojan was detected	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin
1868	Remittance Advice.exe	A Network Trojan was detected	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)
1868	Remittance Advice.exe	A Network Trojan was detected	AV TROJAN Ave Maria RAT CnC Response
1796	Remittance Advice.exe	A Network Trojan was detected	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)
1796	Remittance Advice.exe	A Network Trojan was detected	AV TROJAN Ave Maria RAT CnC Response

Debug output strings

No debug info



Interactive malware hunting service ANY.RUN  
© 2017-2022 ANY.RUN LLC. ALL RIGHTS RESERVED