ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	ხელშეკრულების დოკუმენტი.exe
Full analysis:	https://app.any.run/tasks/1a9d1596-6e43-4297-bbed-f6b79219c055
Verdict:	Malicious activity
Analysis date:	August 19, 2022 at 14:54:14
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5:	E7EEEBF0997168B2A53DB6B4F49FF73D
SHA1:	77B2D72903E4FAFDA700DE58B6803E79F8F8AE21
SHA256:	C2C6DBFB6B0C03A22473C7F2F6CBFE0BBF500C795B920DDEB37C27AF7DE76D93
SSDEEP:	6144:XB+pgULLC8wSCdNcHsJHQ67OVa+ib+2VMo+dMRe/n:XgDL3wdis/7V+ib+8hsv

Software environment set and analysis options

Launch configuration

Task duration:	180 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	120 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
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)
- Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Russian) 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
- KB2685813
- KB2685939
- 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)
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)

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

Loads dropped or rewritten executable
ხელშეკრულების დოკუმენტი.exe (PID: 2628)

Drops executable file immediately after starts
ხელშეკრულების დოკუმენტი.exe (PID: 2628)

SUSPICIOUS

Reads the computer name
ხელშეკრულების დოკუმენტი.exe (PID: 2628)
powershell.exe (PID: 3000)
powershell.exe (PID: 488)
powershell.exe (PID: 2096)
powershell.exe (PID: 2436)
powershell.exe (PID: 1316)
powershell.exe (PID: 3668)
powershell.exe (PID: 3120)
powershell.exe (PID: 324)
powershell.exe (PID: 3472)
powershell.exe (PID: 2492)
powershell.exe (PID: 4052)
powershell.exe (PID: 956)
powershell.exe (PID: 3964)
powershell.exe (PID: 1596)
powershell.exe (PID: 2972)
powershell.exe (PID: 1392)
powershell.exe (PID: 2124)
powershell.exe (PID: 1448)
powershell.exe (PID: 2480)
powershell.exe (PID: 2520)
powershell.exe (PID: 3112)
powershell.exe (PID: 2076)
powershell.exe (PID: 2700)
powershell.exe (PID: 3736)
powershell.exe (PID: 2724)
powershell.exe (PID: 3908)
powershell.exe (PID: 3916)
powershell.exe (PID: 3000)
powershell.exe (PID: 3832)
powershell.exe (PID: 2008)

INFO

Checks Windows Trust Settings
powershell.exe (PID: 3000)
powershell.exe (PID: 2096)
powershell.exe (PID: 488)
powershell.exe (PID: 2436)
powershell.exe (PID: 3120)
powershell.exe (PID: 3668)
powershell.exe (PID: 1316)
powershell.exe (PID: 3472)
powershell.exe (PID: 324)
powershell.exe (PID: 1596)
powershell.exe (PID: 3964)
powershell.exe (PID: 2492)
powershell.exe (PID: 4052)
powershell.exe (PID: 956)
powershell.exe (PID: 1392)
powershell.exe (PID: 2972)
powershell.exe (PID: 2124)
powershell.exe (PID: 1448)
powershell.exe (PID: 2480)
powershell.exe (PID: 2076)
powershell.exe (PID: 3112)
powershell.exe (PID: 2520)
powershell.exe (PID: 2700)
powershell.exe (PID: 3908)
powershell.exe (PID: 3736)
powershell.exe (PID: 3916)
powershell.exe (PID: 3832)
powershell.exe (PID: 2724)
powershell.exe (PID: 3000)
powershell.exe (PID: 2008)
powershell.exe (PID: 4028)

powershell.exe (PID: 3020)
powershell.exe (PID: 4028)
powershell.exe (PID: 1436)
powershell.exe (PID: 2868)
powershell.exe (PID: 2432)
powershell.exe (PID: 1332)
powershell.exe (PID: 2088)
powershell.exe (PID: 3540)
powershell.exe (PID: 952)
powershell.exe (PID: 3504)
powershell.exe (PID: 4040)
powershell.exe (PID: 3680)
powershell.exe (PID: 2748)
powershell.exe (PID: 1304)
powershell.exe (PID: 2440)
powershell.exe (PID: 2132)
powershell.exe (PID: 2676)
powershell.exe (PID: 4064)
powershell.exe (PID: 2696)
powershell.exe (PID: 2776)
powershell.exe (PID: 1168)
powershell.exe (PID: 2848)
powershell.exe (PID: 3572)
powershell.exe (PID: 3816)
powershell.exe (PID: 2540)
powershell.exe (PID: 2384)
powershell.exe (PID: 2592)
powershell.exe (PID: 416)
powershell.exe (PID: 3696)
powershell.exe (PID: 980)
powershell.exe (PID: 1988)
powershell.exe (PID: 464)
powershell.exe (PID: 2132)
powershell.exe (PID: 2904)
powershell.exe (PID: 1468)
powershell.exe (PID: 1116)
powershell.exe (PID: 3028)
powershell.exe (PID: 2692)
powershell.exe (PID: 2756)
powershell.exe (PID: 3052)
powershell.exe (PID: 2352)
powershell.exe (PID: 1572)
powershell.exe (PID: 3248)
powershell.exe (PID: 3212)
powershell.exe (PID: 3868)
powershell.exe (PID: 4016)
powershell.exe (PID: 2072)
powershell.exe (PID: 1144)
powershell.exe (PID: 3416)
powershell.exe (PID: 2472)
powershell.exe (PID: 2432)
powershell.exe (PID: 2120)
powershell.exe (PID: 1180)
powershell.exe (PID: 2096)
powershell.exe (PID: 1360)
powershell.exe (PID: 1076)
powershell.exe (PID: 276)
powershell.exe (PID: 2304)
powershell.exe (PID: 3308)
powershell.exe (PID: 2756)
powershell.exe (PID: 1448)
powershell.exe (PID: 3428)
powershell.exe (PID: 2928)
powershell.exe (PID: 2848)
powershell.exe (PID: 2108)
powershell.exe (PID: 2208)
powershell.exe (PID: 3508)
powershell.exe (PID: 2652)
powershell.exe (PID: 1644)
powershell.exe (PID: 1840)
powershell.exe (PID: 284)
powershell.exe (PID: 2388)
powershell.exe (PID: 4024)
powershell.exe (PID: 356)
powershell.exe (PID: 1196)
powershell.exe (PID: 3140)
powershell.exe (PID: 3996)
powershell.exe (PID: 3960)

Checks supported languages

powershell.exe (PID: 3000)
ხელშეკრულების დოკუმენტი.exe (PID: 2628)
ns6116.tmp (PID: 2832)
ns6427.tmp (PID: 3960)
powershell.exe (PID: 488)
powershell.exe (PID: 2096)
powershell.exe (PID: 3020)
powershell.exe (PID: 2868)
powershell.exe (PID: 2432)
powershell.exe (PID: 2088)
powershell.exe (PID: 1436)
powershell.exe (PID: 3540)
powershell.exe (PID: 1332)
powershell.exe (PID: 4040)
powershell.exe (PID: 952)
powershell.exe (PID: 3504)
powershell.exe (PID: 2748)
powershell.exe (PID: 2440)
powershell.exe (PID: 3680)
powershell.exe (PID: 2132)
powershell.exe (PID: 1304)
powershell.exe (PID: 1168)
powershell.exe (PID: 2676)
powershell.exe (PID: 4064)
powershell.exe (PID: 2776)
powershell.exe (PID: 2696)
powershell.exe (PID: 3572)
powershell.exe (PID: 3816)
powershell.exe (PID: 2540)
powershell.exe (PID: 2848)
powershell.exe (PID: 2384)
powershell.exe (PID: 416)
powershell.exe (PID: 2592)
powershell.exe (PID: 1988)
powershell.exe (PID: 980)
powershell.exe (PID: 3696)
powershell.exe (PID: 1116)
powershell.exe (PID: 2904)
powershell.exe (PID: 1468)
powershell.exe (PID: 3028)
powershell.exe (PID: 2132)
powershell.exe (PID: 464)
powershell.exe (PID: 2352)
powershell.exe (PID: 3052)
powershell.exe (PID: 2756)
powershell.exe (PID: 2692)
powershell.exe (PID: 1572)
powershell.exe (PID: 3212)
powershell.exe (PID: 3248)
powershell.exe (PID: 3868)
powershell.exe (PID: 4016)
powershell.exe (PID: 2072)
powershell.exe (PID: 3416)
powershell.exe (PID: 2432)
powershell.exe (PID: 2472)
powershell.exe (PID: 1144)
powershell.exe (PID: 2120)
powershell.exe (PID: 1180)
powershell.exe (PID: 1360)
powershell.exe (PID: 2096)
powershell.exe (PID: 1076)
powershell.exe (PID: 276)
powershell.exe (PID: 2304)
powershell.exe (PID: 3308)
powershell.exe (PID: 2756)
powershell.exe (PID: 1448)
powershell.exe (PID: 3428)
powershell.exe (PID: 2928)
powershell.exe (PID: 2848)
powershell.exe (PID: 2208)
powershell.exe (PID: 2108)
powershell.exe (PID: 3508)
powershell.exe (PID: 2652)
powershell.exe (PID: 1644)
powershell.exe (PID: 1840)
powershell.exe (PID: 284)
powershell.exe (PID: 2388)
powershell.exe (PID: 4024)
powershell.exe (PID: 356)
powershell.exe (PID: 3960)
powershell.exe (PID: 3140)
powershell.exe (PID: 1196)
powershell.exe (PID: 3996)

powershell.exe (PID: 2436)
ns6572.tmp (PID: 3604)
ns62DD.tmp (PID: 3436)
ns6806.tmp (PID: 1120)
ns66BC.tmp (PID: 2944)
powershell.exe (PID: 1316)
powershell.exe (PID: 3668)
powershell.exe (PID: 3120)
ns6950.tmp (PID: 4040)
ns6BE4.tmp (PID: 2704)
powershell.exe (PID: 3472)
ns6D9C.tmp (PID: 2176)
ns6A9A.tmp (PID: 3808)
powershell.exe (PID: 324)
powershell.exe (PID: 2492)
powershell.exe (PID: 1596)
powershell.exe (PID: 4052)
powershell.exe (PID: 3964)
ns71E7.tmp (PID: 3568)
ns6EE6.tmp (PID: 908)
ns7332.tmp (PID: 4020)
ns747C.tmp (PID: 2220)
ns7030.tmp (PID: 2696)
powershell.exe (PID: 956)
powershell.exe (PID: 2972)
ns75C6.tmp (PID: 2132)
powershell.exe (PID: 1448)
powershell.exe (PID: 2480)
ns79A4.tmp (PID: 1792)
powershell.exe (PID: 1392)
ns7710.tmp (PID: 1980)
ns785A.tmp (PID: 3968)
powershell.exe (PID: 2124)
ns7ECB.tmp (PID: 2072)
powershell.exe (PID: 2700)
powershell.exe (PID: 2520)
ns7D13.tmp (PID: 1972)
powershell.exe (PID: 3112)
ns8082.tmp (PID: 2452)
powershell.exe (PID: 2076)
ns7B5C.tmp (PID: 2824)
ns81CC.tmp (PID: 3184)
ns8384.tmp (PID: 3520)
powershell.exe (PID: 3736)
powershell.exe (PID: 3916)
ns853B.tmp (PID: 2552)
powershell.exe (PID: 3908)
ns86F3.tmp (PID: 1312)
powershell.exe (PID: 2724)
powershell.exe (PID: 3000)
ns88AA.tmp (PID: 852)
ns8A62.tmp (PID: 628)
powershell.exe (PID: 3832)
ns8C19.tmp (PID: 1168)
ns8F1B.tmp (PID: 3432)
powershell.exe (PID: 3020)
powershell.exe (PID: 2008)
powershell.exe (PID: 4028)
ns8DD1.tmp (PID: 2676)
ns90D2.tmp (PID: 3924)
powershell.exe (PID: 2868)
powershell.exe (PID: 2432)
powershell.exe (PID: 2088)
ns97B0.tmp (PID: 1108)
ns928A.tmp (PID: 1720)
powershell.exe (PID: 1436)
ns9441.tmp (PID: 2392)
ns95F9.tmp (PID: 3076)
powershell.exe (PID: 3540)
ns9DB4.tmp (PID: 756)
ns9AB2.tmp (PID: 2296)
ns9968.tmp (PID: 128)
powershell.exe (PID: 1332)
powershell.exe (PID: 952)
ns9C6A.tmp (PID: 3548)
powershell.exe (PID: 3504)
ns9EFE.tmp (PID: 2556)
powershell.exe (PID: 4040)
nsA2DC.tmp (PID: 1360)
powershell.exe (PID: 2748)
powershell.exe (PID: 1304)
powershell.exe (PID: 2132)
powershell.exe (PID: 3680)
powershell.exe (PID: 2440)
nsA570.tmp (PID: 1176)

nsA192.tmp (PID: 1180)
nsA048.tmp (PID: 2992)
nsA426.tmp (PID: 2588)
powershell.exe (PID: 2696)
nsA6BB.tmp (PID: 2352)
powershell.exe (PID: 3572)
nsA805.tmp (PID: 3900)
powershell.exe (PID: 4064)
powershell.exe (PID: 2676)
powershell.exe (PID: 1168)
nsABE3.tmp (PID: 1448)
powershell.exe (PID: 2776)
nsA94F.tmp (PID: 1960)
nsAA99.tmp (PID: 3480)
powershell.exe (PID: 3816)
nsAE77.tmp (PID: 2504)
powershell.exe (PID: 2848)
powershell.exe (PID: 416)
nsAFC1.tmp (PID: 3488)
powershell.exe (PID: 2540)
powershell.exe (PID: 2384)
nsB10C.tmp (PID: 3988)
nsAD2D.tmp (PID: 2108)
nsB256.tmp (PID: 3948)
nsB40D.tmp (PID: 2400)
nsB9A3.tmp (PID: 2488)
nsB557.tmp (PID: 3016)
nsB6A1.tmp (PID: 3776)
powershell.exe (PID: 3696)
nsB7EC.tmp (PID: 2612)
powershell.exe (PID: 1988)
powershell.exe (PID: 2592)
powershell.exe (PID: 980)
powershell.exe (PID: 464)
nsBB5B.tmp (PID: 3168)
powershell.exe (PID: 2132)
powershell.exe (PID: 1468)
powershell.exe (PID: 1116)
nsBF39.tmp (PID: 3764)
nsC083.tmp (PID: 276)
nsBCA5.tmp (PID: 2680)
powershell.exe (PID: 2904)
nsBDEF.tmp (PID: 2552)
powershell.exe (PID: 2756)
nsC6F6.tmp (PID: 3700)
powershell.exe (PID: 3052)
nsC461.tmp (PID: 2720)
nsC1CD.tmp (PID: 1540)
powershell.exe (PID: 2692)
powershell.exe (PID: 2352)
powershell.exe (PID: 3028)
nsC317.tmp (PID: 3704)
nsC5AC.tmp (PID: 2908)
powershell.exe (PID: 1572)
powershell.exe (PID: 3248)
powershell.exe (PID: 3212)
nsC840.tmp (PID: 1948)
nsC9F7.tmp (PID: 1760)
nsCB41.tmp (PID: 3064)
powershell.exe (PID: 3868)
nsCC8C.tmp (PID: 280)
powershell.exe (PID: 4016)
nsCDD6.tmp (PID: 2068)
powershell.exe (PID: 2072)
nsD06A.tmp (PID: 400)
powershell.exe (PID: 3416)
nsCF20.tmp (PID: 3008)
powershell.exe (PID: 1144)
nsD221.tmp (PID: 980)
powershell.exe (PID: 2472)
powershell.exe (PID: 2432)
nsD36C.tmp (PID: 1244)
nsD4B6.tmp (PID: 3260)
powershell.exe (PID: 2120)
nsD74A.tmp (PID: 4052)
powershell.exe (PID: 1180)
nsD600.tmp (PID: 1472)
powershell.exe (PID: 1360)
nsD894.tmp (PID: 3528)
nsD9DE.tmp (PID: 484)
powershell.exe (PID: 2096)
powershell.exe (PID: 1076)
nsDB28.tmp (PID: 3548)
powershell.exe (PID: 276)
powershell.exe (PID: 2304)

nsDC72.tmp (PID: 2444)
nsDDBD.tmp (PID: 1708)
powershell.exe (PID: 2756)
nsDF07.tmp (PID: 2868)
powershell.exe (PID: 3308)
nsE051.tmp (PID: 460)
powershell.exe (PID: 1448)
nsE19B.tmp (PID: 2680)
powershell.exe (PID: 3428)
nsE2E5.tmp (PID: 2852)
powershell.exe (PID: 2928)
nsE49D.tmp (PID: 3320)
powershell.exe (PID: 2848)
nsE5E7.tmp (PID: 1116)
nsE731.tmp (PID: 2352)
powershell.exe (PID: 2108)
powershell.exe (PID: 2208)
nsE87B.tmp (PID: 4028)
powershell.exe (PID: 3508)
nsEA32.tmp (PID: 1496)
powershell.exe (PID: 2652)
nsEBEA.tmp (PID: 2300)
powershell.exe (PID: 1644)
nsED34.tmp (PID: 1332)
powershell.exe (PID: 1840)
nsEE7E.tmp (PID: 3704)
powershell.exe (PID: 284)
powershell.exe (PID: 2388)
nsEFC8.tmp (PID: 3752)
nsF112.tmp (PID: 3028)
powershell.exe (PID: 4024)
nsF3A7.tmp (PID: 3276)
nsF25D.tmp (PID: 280)
powershell.exe (PID: 356)
nsF4F1.tmp (PID: 2480)
powershell.exe (PID: 3140)
powershell.exe (PID: 1196)
nsF860.tmp (PID: 2728)
powershell.exe (PID: 3960)
nsF6A8.tmp (PID: 4020)
powershell.exe (PID: 3996)

Starts application with an unusual extension
ხელშეკრულების დოკუმენტი.exe (PID: 2628)

Executable content was dropped or overwritten
ხელშეკრულების დოკუმენტი.exe (PID: 2628)

Drops a file with a compile date too recent
ხელშეკრულების დოკუმენტი.exe (PID: 2628)

Static information

TRiD

.exe | Win32 Executable MS Visual C++ (generic) (42.2)
.exe | Win64 Executable (generic) (37.3)
.dll | Win32 Dynamic Link Library (generic) (8.8)
.exe | Win32 Executable (generic) (6)
.exe | Generic Win/DOS Executable (2.7)

EXIF

EXE

Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	6
OSVersion:	4
EntryPoint:	0x33b6
UninitializedDataSize:	2048
InitializedDataSize:	141824
CodeSize:	25088
LinkerVersion:	6
PEType:	PE32
TimeStamp:	2016:07:25 02:55:51+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	25-Jul-2016 00:55:51
Detected languages:	English - United States

DOS Header

Magic number:	MZ

PE Headers

Signature:	PE

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
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:	0x000000C8

Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	5
Time date stamp:	25-Jul-2016 00:55:51
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LINE_NUMS_STRIPPED IMAGE_FILE_LOCAL_SYMS_STRIPPED IMAGE_FILE_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x0000615D	0x00006200	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.45023
.rdata	0x00008000	0x000013A4	0x00001400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.163
.data	0x0000A000	0x00020338	0x00000600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	3.9824
.ndata	0x0002B000	0x00033000	0x00000000	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rsrc	0x0005E000	0x000198A8	0x00019A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	2.39671

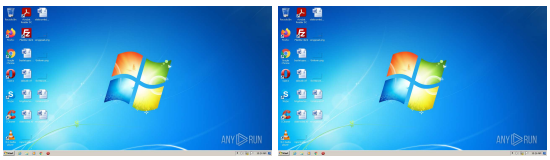
Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.29829	829	UNKNOWN	English - United States	RT_MANIFEST
2	5.10733	16936	UNKNOWN	English - United States	RT_ICON
3	5.16619	9640	UNKNOWN	English - United States	RT_ICON
4	5.35415	4264	UNKNOWN	English - United States	RT_ICON
5	5.47079	2440	UNKNOWN	English - United States	RT_ICON
6	5.17786	1128	UNKNOWN	English - United States	RT_ICON
103	2.93166	90	UNKNOWN	English - United States	RT_GROUP_ICON
105	2.66174	256	UNKNOWN	English - United States	RT_DIALOG
106	2.88094	284	UNKNOWN	English - United States	RT_DIALOG
111	2.48825	96	UNKNOWN	English - United States	RT_DIALOG

Imports

ADVAPI32.dll
COMCTL32.dll
GDI32.dll
KERNEL32.dll
SHELL32.dll
USER32.dll
ole32.dll

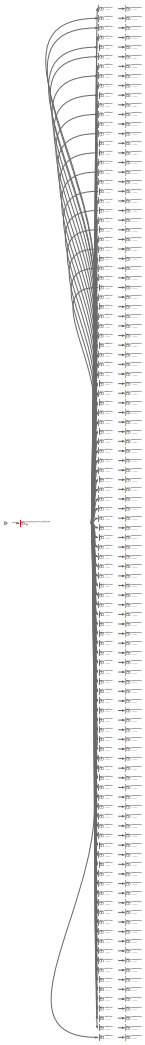
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
357	217	1	108

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
2628	"C:\Users\admin\AppData\Local\Temp\ხელშეკრულების დოკუმენტი.exe"	C:\Users\admin\AppData\Local\Temp\ხელშეკრულების დოკუმენტი.exe		Explorer.EXE
	Information			
	User: admin **Integrity Level:** MEDIUM			
2832	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6116.tmp" powershell.exe icm -ScriptBlock{0x65 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6116.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

3000	powershell.exe icm -ScriptBlock{0x65 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6116.tmp

Information

User: admin Company: Microsoft Corporation

Integrity Level: MEDIUM Description: Windows PowerShell

Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3436	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns62DD.tmp" powershell.exe icm -ScriptBlock{0x6B -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns62DD.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

488	powershell.exe icm -ScriptBlock{0x6B -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns62DD.tmp

Information

User: admin Company: Microsoft Corporation

Integrity Level: MEDIUM Description: Windows PowerShell

Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3960	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6427.tmp" powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6427.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

2096	powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6427.tmp

Information

User: admin Company: Microsoft Corporation

Integrity Level: MEDIUM Description: Windows PowerShell

Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3604	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6572.tmp" powershell.exe icm -ScriptBlock{0x60 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6572.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

2436	powershell.exe icm -ScriptBlock{0x60 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6572.tmp

Information

User: admin Company: Microsoft Corporation

Integrity Level: MEDIUM Description: Windows PowerShell

Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2944	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns66BC.tmp" powershell.exe icm -ScriptBlock{0x6B -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns66BC.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

3120	powershell.exe icm -ScriptBlock{0x6B -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns66BC.tmp

Information

User: admin Company: Microsoft Corporation

Integrity Level: MEDIUM Description: Windows PowerShell

Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

1120	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6806.tmp" powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6806.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

3668	powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6806.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

4040	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6950.tmp" powershell.exe icm -ScriptBlock{0x3D -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6950.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1316	powershell.exe icm -ScriptBlock{0x3D -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6950.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3808	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6A9A.tmp" powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6A9A.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

324	powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6A9A.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2704	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6BE4.tmp" powershell.exe icm -ScriptBlock{0x34 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6BE4.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3472	powershell.exe icm -ScriptBlock{0x34 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6BE4.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2176	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6D9C.tmp" powershell.exe icm -ScriptBlock{0x34 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6D9C.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2492	powershell.exe icm -ScriptBlock{0x34 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6D9C.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

908	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6EE6.tmp" powershell.exe icm -ScriptBlock{0x58 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6EE6.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

4052	powershell.exe icm -ScriptBlock{0x58 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns6EE6.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2696	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7030.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7030.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1596	powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns7030.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3568	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns71E7.tmp" powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns71E7.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

956	powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns71E7.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

4020	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7332.tmp" powershell.exe icm -ScriptBlock{0x7A -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7332.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3964	powershell.exe icm -ScriptBlock{0x7A -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns7332.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2220	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns747C.tmp" powershell.exe icm -ScriptBlock{0x7B -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns747C.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1392	powershell.exe icm -ScriptBlock{0x7B -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns747C.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2132	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns75C6.tmp" powershell.exe icm -ScriptBlock{0x6F -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns75C6.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2972	powershell.exe icm -ScriptBlock{0x6F -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns75C6.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1980	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7710.tmp" powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7710.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

1448	powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns7710.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3968	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns785A.tmp" powershell.exe icm -ScriptBlock{0x4F -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns785A.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2124	powershell.exe icm -ScriptBlock{0x4F -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns785A.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1792	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns79A4.tmp" powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns79A4.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2480	powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns79A4.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2824	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7B5C.tmp" powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7B5C.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2520	powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns7B5C.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1972	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7D13.tmp" powershell.exe icm -ScriptBlock{0x61 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7D13.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3112	powershell.exe icm -ScriptBlock{0x61 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns7D13.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2072	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7ECB.tmp" powershell.exe icm -ScriptBlock{0x6D -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7ECB.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2076 powershell.exe icm -ScriptBlock{0x6D -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — ns7ECB.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2452 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8082.tmp" powershell.exe icm -ScriptBlock{0x4B -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8082.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2700 powershell.exe icm -ScriptBlock{0x4B -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — ns8082.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3184 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns81CC.tmp" powershell.exe icm -ScriptBlock{0x76 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns81CC.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3736 powershell.exe icm -ScriptBlock{0x76 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — ns81CC.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3520 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8384.tmp" powershell.exe icm -ScriptBlock{0x26 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8384.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3908 powershell.exe icm -ScriptBlock{0x26 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — ns8384.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2552 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns853B.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns853B.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3916 powershell.exe icm -ScriptBlock{0x67 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — ns853B.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

1312 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns86F3.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns86F3.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2724	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns86F3.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

852	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns88AA.tmp" powershell.exe icm -ScriptBlock{0x23 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns88AA.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3000	powershell.exe icm -ScriptBlock{0x23 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns88AA.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

628	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8A62.tmp" powershell.exe icm -ScriptBlock{0x3F -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8A62.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3832	powershell.exe icm -ScriptBlock{0x3F -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns8A62.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1168	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8C19.tmp" powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8C19.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2008	powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns8C19.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2676	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8DD1.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8DD1.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

4028	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns8DD1.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3432	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8F1B.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8F1B.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3020	powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns8F1B.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3924	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns90D2.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns90D2.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2088	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns90D2.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1720	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns928A.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns928A.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2432	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns928A.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2392	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9441.tmp" powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9441.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2868	powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns9441.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3076	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns95F9.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns95F9.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1436	powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns95F9.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1108	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns97B0.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns97B0.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1332	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns97B0.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

128	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9968.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9968.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

4040	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns9968.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2296	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9AB2.tmp" powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9AB2.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3540	powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns9AB2.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3548	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9C6A.tmp" powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9C6A.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3504	powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns9C6A.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

756	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9DB4.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9DB4.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

952	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns9DB4.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2556	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9EFE.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9EFE.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3680	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	ns9EFE.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2992	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA048.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA048.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM
Exit code: 0

2748	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA048.tmp

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Windows PowerShell
Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1180	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA192.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA192.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM
Exit code: 0

2132	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA192.tmp

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Windows PowerShell
Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1360	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA2DC.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA2DC.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM
Exit code: 0

1304	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA2DC.tmp

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Windows PowerShell
Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2588	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA426.tmp" powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA426.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM
Exit code: 0

2440	powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA426.tmp

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Windows PowerShell
Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1176	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA570.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA570.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM
Exit code: 0

2696	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA570.tmp

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Windows PowerShell
Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2352	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA6BB.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA6BB.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM
Exit code: 0

2776	powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA6BB.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3900	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA805.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA805.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

4064	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA805.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1960	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA94F.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA94F.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1168	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsA94F.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3480	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAA99.tmp" powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAA99.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2676	powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsAA99.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1448	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsABE3.tmp" powershell.exe icm -ScriptBlock{0x3D -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsABE3.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3572	powershell.exe icm -ScriptBlock{0x3D -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsABE3.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2108	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAD2D.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAD2D.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2540	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsAD2D.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2504 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAE77.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAE77.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2848 powershell.exe icm -ScriptBlock{0x3E -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsAE77.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3488 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAFC1.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAFC1.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3816 powershell.exe icm -ScriptBlock{0x3E -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsAFC1.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3988 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB10C.tmp" powershell.exe icm -ScriptBlock{0x22 -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB10C.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2384 powershell.exe icm -ScriptBlock{0x22 -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsB10C.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3948 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB256.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB256.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

416 powershell.exe icm -ScriptBlock{0x2E -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsB256.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2400 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB40D.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB40D.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2592 powershell.exe icm -ScriptBlock{0x67 -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsB40D.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3016	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB557.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB557.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3696	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsB557.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3776	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB6A1.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB6A1.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

980	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsB6A1.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2612	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB7EC.tmp" powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB7EC.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

1988	powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsB7EC.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2488	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB9A3.tmp" powershell.exe icm -ScriptBlock{0x3A -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB9A3.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

464	powershell.exe icm -ScriptBlock{0x3A -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsB9A3.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3168	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBB5B.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBB5B.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

1116	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsBB5B.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2680	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBCA5.tmp" powershell.exe icm -ScriptBlock{0x27 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBCA5.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2132 powershell.exe icm -ScriptBlock{0x27 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsBCA5.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2552 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBDEF.tmp" powershell.exe icm -ScriptBlock{0x7E -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBDEF.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

1468 powershell.exe icm -ScriptBlock{0x7E -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsBDEF.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3764 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBF39.tmp" powershell.exe icm -ScriptBlock{0x20 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBF39.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2904 powershell.exe icm -ScriptBlock{0x20 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsBF39.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

276 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC083.tmp" powershell.exe icm -ScriptBlock{0x7C -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC083.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3028 powershell.exe icm -ScriptBlock{0x7C -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsC083.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

1540 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC1CD.tmp" powershell.exe icm -ScriptBlock{0x3C -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC1CD.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2352 powershell.exe icm -ScriptBlock{0x3C -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsC1CD.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3704 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC317.tmp" powershell.exe icm -ScriptBlock{0x45 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC317.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2756	powershell.exe icm -ScriptBlock{0x45 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsC317.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2720	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC461.tmp" powershell.exe icm -ScriptBlock{0x4B -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC461.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2692	powershell.exe icm -ScriptBlock{0x4B -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsC461.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2908	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC5AC.tmp" powershell.exe icm -ScriptBlock{0x5C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC5AC.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3052	powershell.exe icm -ScriptBlock{0x5C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsC5AC.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3700	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC6F6.tmp" powershell.exe icm -ScriptBlock{0x40 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC6F6.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1572	powershell.exe icm -ScriptBlock{0x40 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsC6F6.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1948	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC840.tmp" powershell.exe icm -ScriptBlock{0x4B -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC840.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3212	powershell.exe icm -ScriptBlock{0x4B -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsC840.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1760	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC9F7.tmp" powershell.exe icm -ScriptBlock{0x42 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC9F7.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3248	powershell.exe icm -ScriptBlock{0x42 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsC9F7.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3064 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCB41.tmp" powershell.exe icm -ScriptBlock{0x3D -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCB41.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3868 powershell.exe icm -ScriptBlock{0x3D -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsCB41.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

280 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCC8C.tmp" powershell.exe icm -ScriptBlock{0x3C -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCC8C.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

4016 powershell.exe icm -ScriptBlock{0x3C -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsCC8C.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2068 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCDD6.tmp" powershell.exe icm -ScriptBlock{0x34 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCDD6.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2072 powershell.exe icm -ScriptBlock{0x34 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsCDD6.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3008 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCF20.tmp" powershell.exe icm -ScriptBlock{0x34 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCF20.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3416 powershell.exe icm -ScriptBlock{0x34 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsCF20.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

400 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD06A.tmp" powershell.exe icm -ScriptBlock{0x51 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD06A.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1144 powershell.exe icm -ScriptBlock{0x51 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsD06A.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

980	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD221.tmp" powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD221.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2472	powershell.exe icm -ScriptBlock{0x62 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsD221.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1244	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD36C.tmp" powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD36C.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2432	powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsD36C.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3260	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD4B6.tmp" powershell.exe icm -ScriptBlock{0x6B -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD4B6.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2120	powershell.exe icm -ScriptBlock{0x6B -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsD4B6.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

1472	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD600.tmp" powershell.exe icm -ScriptBlock{0x6F -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD600.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

1180	powershell.exe icm -ScriptBlock{0x6F -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsD600.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

4052	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD74A.tmp" powershell.exe icm -ScriptBlock{0x6A -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD74A.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

1360	powershell.exe icm -ScriptBlock{0x6A -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsD74A.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3528	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD894.tmp" powershell.exe icm -ScriptBlock{0x26 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD894.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2096 powershell.exe icm -ScriptBlock{0x26 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsD894.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

484 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD9DE.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD9DE.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

1076 powershell.exe icm -ScriptBlock{0x67 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsD9DE.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

3548 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDB28.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDB28.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

276 powershell.exe icm -ScriptBlock{0x2E -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsDB28.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2444 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDC72.tmp" powershell.exe icm -ScriptBlock{0x7C -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDC72.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2304 powershell.exe icm -ScriptBlock{0x7C -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsDC72.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

1708 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDDBD.tmp" powershell.exe icm -ScriptBlock{0x3B -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDDBD.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

2756 powershell.exe icm -ScriptBlock{0x3B -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsDDBD.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2868 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDF07.tmp" powershell.exe icm -ScriptBlock{0x22 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDF07.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3308	powershell.exe icm -ScriptBlock{0x22 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsDF07.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

460	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE051.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE051.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1448	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsE051.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2680	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE19B.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE19B.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3428	powershell.exe icm -ScriptBlock{0x67 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsE19B.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2852	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE2E5.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE2E5.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2928	powershell.exe icm -ScriptBlock{0x2E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsE2E5.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3320	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE49D.tmp" powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE49D.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2848	powershell.exe icm -ScriptBlock{0x7C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsE49D.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1116	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE5E7.tmp" powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE5E7.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2208	powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsE5E7.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2352 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE731.tmp" powershell.exe icm -ScriptBlock{0x22 -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE731.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2108 powershell.exe icm -ScriptBlock{0x22 -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsE731.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

4028 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE87B.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE87B.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

3508 powershell.exe icm -ScriptBlock{0x2E -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsE87B.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1496 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEA32.tmp" powershell.exe icm -ScriptBlock{0x67 -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEA32.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

2652 powershell.exe icm -ScriptBlock{0x67 -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsEA32.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

2300 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEBEA.tmp" powershell.exe icm -ScriptBlock{0x2E -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEBEA.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1644 powershell.exe icm -ScriptBlock{0x2E -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsEBEA.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

1332 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsED34.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14} | C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsED34.tmp | — | ხელშეკრულების დოკუმენტი.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Exit code:	0		

1840 powershell.exe icm -ScriptBlock{0x3E -bxor 14} | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | — | nsED34.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3704	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEE7E.tmp" powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEE7E.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

284	powershell.exe icm -ScriptBlock{0x76 -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsEE7E.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3752	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEFC8.tmp" powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEFC8.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

2388	powershell.exe icm -ScriptBlock{0x3C -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsEFC8.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3028	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF112.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF112.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

4024	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsF112.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

280	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF25D.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF25D.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

356	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsF25D.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

3276	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF3A7.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF3A7.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3140	powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	nsF3A7.tmp

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows PowerShell

Exit code: 0 **Version:** 10.0.14409.1005 (rs1_srvoob.161208-1155)

2480	"C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF4F1.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14}	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF4F1.tmp	—	ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3960 powershell.exe icm -ScriptBlock{0x3E -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsF4F1.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

4020 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF6A8.tmp" powershell.exe icm -ScriptBlock{0x3E -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF6A8.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

1196 powershell.exe icm -ScriptBlock{0x3E -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsF6A8.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

2728 "C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF860.tmp" powershell.exe icm -ScriptBlock{0x27 -bxor 14} C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF860.tmp — ხელშეკრულების დოკუმენტი.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

3996 powershell.exe icm -ScriptBlock{0x27 -bxor 14} C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — nsF860.tmp

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Windows PowerShell
Exit code: 0 Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

Registry activity

Total events	Read events	Write events	Delete events
56 817	56 814	3	0

Modification events

(PID) Process: (2628) ხელშეკრულების დოკუმენტი.exe Key: HKEY_CURRENT_USER\Software\Krminde
Operation: write Name: juts
Value: %WINDIR%\Krebsenes\Nondecreasing\Camphine\Doncella.Sus

Files activity

Executable files	Suspicious files	Text files	Unknown types
111	217	0	1

Dropped files

PID	Process	Filename	Type
3000	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive MD5: 446DD1CF97EABA21CF14D03AEBC79F27 SHA256: A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF	dbf
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\System.dll MD5: A4DD044BCD94E9B3370CCF095B31F896 SHA256: 2E226715419A5882E2E14278940EE8EF0AA648A3EF7AF5B3DC252674111962BC	executable
2628	ხელშეკრულების	C:\Users\admin\AppData\Roaming\Krakeleringerne19\Ferskvareterminalernes\Crags\rgningers\Columnists\Galactosamine\ArmouryCrate.Deno	executable

	დოკუმენტი.exe	iseAI.exe **MD5:** 33A476011F2D0D129FC48C9F75FFC462 **SHA256:** B92F001E77272414DEA2915A6D66C2C015210EB53323E60A3DB00283B80FB0C2	
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6572.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Roaming\Krakeleringerne19\Ferskvareterminalernes\Crags\Rytmesektion167\Prvekonverteringerne\Aftopninger\Pythia\Kursusoversigten194.Sta **MD5:** EBEAE5A3C49C11A7F34DD8E0916021EA **SHA256:** A1B38A0B0EF9C768D740B74FC452DEF9654D3FA34602C47BE0466BD3AB32CA74	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns66BC.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
3000	powershell.exe	C:\Users\admin\AppData\Local\Temp\ga3zjyoy.yns.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns62DD.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
488	powershell.exe	C:\Users\admin\AppData\Local\Temp\a1rbmzqv.fjl.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
488	powershell.exe	C:\Users\admin\AppData\Local\Temp\grmn51gw.enb.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6116.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2096	powershell.exe	C:\Users\admin\AppData\Local\Temp\azp5jlx4.4z4.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3000	powershell.exe	C:\Users\admin\AppData\Local\Temp\otu51prl.ex2.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2096	powershell.exe	C:\Users\admin\AppData\Local\Temp\3ohxrm4h.pjr.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3120	powershell.exe	C:\Users\admin\AppData\Local\Temp\udvnvp13.nsb.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsExec.dll **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2436	powershell.exe	C:\Users\admin\AppData\Local\Temp\zn2vhnhp.eda.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3120	powershell.exe	C:\Users\admin\AppData\Local\Temp\axtpn4as.ej4.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6427.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2436	powershell.exe	C:\Users\admin\AppData\Local\Temp\ecg50yag.1bc.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3668	powershell.exe	C:\Users\admin\AppData\Local\Temp\atj5q2in.mub.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1316	powershell.exe	C:\Users\admin\AppData\Local\Temp\tuh505jt.yoc.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6806.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
1316	powershell.exe	C:\Users\admin\AppData\Local\Temp\nbkq2n2f.rst.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6BE4.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
324	powershell.exe	C:\Users\admin\AppData\Local\Temp\dihavr3b.zah.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6A9A.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
3668	powershell.exe	C:\Users\admin\AppData\Local\Temp\0lahnsob.rgy.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
324	powershell.exe	C:\Users\admin\AppData\Local\Temp\kvb5oe5m.nhm.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6950.tmp	executable

	დოკუმენტი.exe	**MD5:** C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
4052	powershell.exe	C:\Users\admin\AppData\Local\Temp\1a2ya2gy.f4q.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3472	powershell.exe	C:\Users\admin\AppData\Local\Temp\eyw5535a.i5t.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1596	powershell.exe	C:\Users\admin\AppData\Local\Temp\t053moto.4cm.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7030.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2492	powershell.exe	C:\Users\admin\AppData\Local\Temp\fctgjfmx.eg1.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3472	powershell.exe	C:\Users\admin\AppData\Local\Temp\ethqoe50.bne.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1596	powershell.exe	C:\Users\admin\AppData\Local\Temp\fu3fk1nk.yux.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6EE6.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns6D9C.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2492	powershell.exe	C:\Users\admin\AppData\Local\Temp\q2iyyhl5.xuf.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4052	powershell.exe	C:\Users\admin\AppData\Local\Temp\itgqj1ag.msl.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
956	powershell.exe	C:\Users\admin\AppData\Local\Temp\mr5rouid.lzi.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns747C.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2972	powershell.exe	C:\Users\admin\AppData\Local\Temp\r3k35smy.aji.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns71E7.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1392	powershell.exe	C:\Users\admin\AppData\Local\Temp\1miyfloy.tar.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3964	powershell.exe	C:\Users\admin\AppData\Local\Temp\4abdhh5r.mzv.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7332.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2972	powershell.exe	C:\Users\admin\AppData\Local\Temp\o5x3eeiu.m2z.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns75C6.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426	executable **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
956	powershell.exe	C:\Users\admin\AppData\Local\Temp\dytcgiu5.u10.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3964	powershell.exe	C:\Users\admin\AppData\Local\Temp\jearqn1t.1ty.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1392	powershell.exe	C:\Users\admin\AppData\Local\Temp\jrungfdm.kep.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2480	powershell.exe	C:\Users\admin\AppData\Local\Temp\mgwzjxwb.ba0.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2124	powershell.exe	C:\Users\admin\AppData\Local\Temp\hidejwmo.bmg.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1448	powershell.exe	C:\Users\admin\AppData\Local\Temp\mttxckzw.xd5.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B	binary **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns79A4.tmp	executable

		MD5: C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	
2124	powershell.exe	C:\Users\admin\AppData\Local\Temp\ierg3c0h.naz.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1448	powershell.exe	C:\Users\admin\AppData\Local\Temp\thqklrzq.htw.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns785A.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7B5C.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7710.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2480	powershell.exe	C:\Users\admin\AppData\Local\Temp\eoszksyj.qpo.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2520	powershell.exe	C:\Users\admin\AppData\Local\Temp\gu5bsznj.mgf.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3112	powershell.exe	C:\Users\admin\AppData\Local\Temp\lhx1s4ex.zyv.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2520	powershell.exe	C:\Users\admin\AppData\Local\Temp\nnfhsdpm.m0k.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8082.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2076	powershell.exe	C:\Users\admin\AppData\Local\Temp\eanfvfu2.scz.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7ECB.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
3112	powershell.exe	C:\Users\admin\AppData\Local\Temp\jwlakwmk.lft.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns7D13.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2700	powershell.exe	C:\Users\admin\AppData\Local\Temp\w3aood3j.xvx.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2076	powershell.exe	C:\Users\admin\AppData\Local\Temp\mcfvscyu.w01.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8384.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2724	powershell.exe	C:\Users\admin\AppData\Local\Temp\pf1bhsfo.cyn.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3908	powershell.exe	C:\Users\admin\AppData\Local\Temp\3eu5cxwr.cgy.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns81CC.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns86F3.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns853B.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
3736	powershell.exe	C:\Users\admin\AppData\Local\Temp\c3u1qzqv.ons.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3916	powershell.exe	C:\Users\admin\AppData\Local\Temp\0o5iwqcs.yzr.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2700	powershell.exe	C:\Users\admin\AppData\Local\Temp\u30l1p1j.egh.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2724	powershell.exe	C:\Users\admin\AppData\Local\Temp\wtrh54wn.kw3.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3736	powershell.exe	C:\Users\admin\AppData\Local\Temp\zh3xzm1h.h0q.ps1	binary

		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3916	powershell.exe	C:\Users\admin\AppData\Local\Temp\yho14ggq.srs.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns88AA.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3908	powershell.exe	C:\Users\admin\AppData\Local\Temp\hpunt2xe.swp.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2008	powershell.exe	C:\Users\admin\AppData\Local\Temp\54tzrm0w.3io.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3832	powershell.exe	C:\Users\admin\AppData\Local\Temp\q5zzn1l0.ubd.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3000	powershell.exe	C:\Users\admin\AppData\Local\Temp\r1w0yuqj.dih.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8C19.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3832	powershell.exe	C:\Users\admin\AppData\Local\Temp\1hoqptv1.y01.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2008	powershell.exe	C:\Users\admin\AppData\Local\Temp\ltsrzqvr.pcw.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3000	powershell.exe	C:\Users\admin\AppData\Local\Temp\wksditz4.e1y.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8A62.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
4028	powershell.exe	C:\Users\admin\AppData\Local\Temp\lxs3w2lu.3ty.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8F1B.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3020	powershell.exe	C:\Users\admin\AppData\Local\Temp\c3qxplsr.jmv.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4028	powershell.exe	C:\Users\admin\AppData\Local\Temp\hn5uxilh.lao.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3020	powershell.exe	C:\Users\admin\AppData\Local\Temp\mnxomjaa.wly.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns8DD1.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns90D2.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2432	powershell.exe	C:\Users\admin\AppData\Local\Temp\yuypl2cg.yol.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2088	powershell.exe	C:\Users\admin\AppData\Local\Temp\l5czg5gh.t5j.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2088	powershell.exe	C:\Users\admin\AppData\Local\Temp\ijzc2l4g.y2p.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns928A.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2432	powershell.exe	C:\Users\admin\AppData\Local\Temp\jvccktwt.42e.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1436	powershell.exe	C:\Users\admin\AppData\Local\Temp\geiqqg2t.g51.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1436	powershell.exe	C:\Users\admin\AppData\Local\Temp\smdckoyu.332.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9441.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2868	powershell.exe	C:\Users\admin\AppData\Local\Temp\lqccuepv.u1o.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

2868	powershell.exe	C:\Users\admin\AppData\Local\Temp\0ch3a4v2.a3v.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns95F9.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1332	powershell.exe	C:\Users\admin\AppData\Local\Temp\0mjcxsfh.qie.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9AB2.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1332	powershell.exe	C:\Users\admin\AppData\Local\Temp\fcpt1cuu.tm4.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns97B0.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9C6A.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3504	powershell.exe	C:\Users\admin\AppData\Local\Temp\wi41xgnd.u42.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3540	powershell.exe	C:\Users\admin\AppData\Local\Temp\b5q42otr.hft.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4040	powershell.exe	C:\Users\admin\AppData\Local\Temp\iqjgdxlo.fdv.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3504	powershell.exe	C:\Users\admin\AppData\Local\Temp\jl01hh1r.uw4.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4040	powershell.exe	C:\Users\admin\AppData\Local\Temp\kfqcnjk5.1r1.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
952	powershell.exe	C:\Users\admin\AppData\Local\Temp\e4ytouoh.0je.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9DB4.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9968.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3540	powershell.exe	C:\Users\admin\AppData\Local\Temp\2mx04ibe.km3.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
952	powershell.exe	C:\Users\admin\AppData\Local\Temp\reqzsjbn.vpu.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA192.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\ns9EFE.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3680	powershell.exe	C:\Users\admin\AppData\Local\Temp\t4glbgiz.kq2.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2748	powershell.exe	C:\Users\admin\AppData\Local\Temp\ukxvbarl.i2p.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2132	powershell.exe	C:\Users\admin\AppData\Local\Temp\barvfsjh.hcp.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA2DC.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA048.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1304	powershell.exe	C:\Users\admin\AppData\Local\Temp\wqm51wmp.epp.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1304	powershell.exe	C:\Users\admin\AppData\Local\Temp\2gyvsulp.l25.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2132	powershell.exe	C:\Users\admin\AppData\Local\Temp\h2tefbuh.bcg.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

2748	powershell.exe	C:\Users\admin\AppData\Local\Temp\2bkwonsc.kcf.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3680	powershell.exe	C:\Users\admin\AppData\Local\Temp\uakeeoyu.bai.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA426.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2440	powershell.exe	C:\Users\admin\AppData\Local\Temp\tt442ndn.aqt.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA570.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA6BB.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2696	powershell.exe	C:\Users\admin\AppData\Local\Temp\dpeorotk.31z.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAA99.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA94F.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2776	powershell.exe	C:\Users\admin\AppData\Local\Temp\0htsoe3z.c3h.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2696	powershell.exe	C:\Users\admin\AppData\Local\Temp\f2ie1lst.by4.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1168	powershell.exe	C:\Users\admin\AppData\Local\Temp\y4n3xr3a.tdi.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
4064	powershell.exe	C:\Users\admin\AppData\Local\Temp\51ba51zd.1tp.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
4064	powershell.exe	C:\Users\admin\AppData\Local\Temp\m0r45ods.2r5.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2440	powershell.exe	C:\Users\admin\AppData\Local\Temp\lqziaym1.3xa.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1168	powershell.exe	C:\Users\admin\AppData\Local\Temp\ghkc2lbg.fjt.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsA805.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2776	powershell.exe	C:\Users\admin\AppData\Local\Temp\z4lhomrk.vzw.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2676	powershell.exe	C:\Users\admin\AppData\Local\Temp\ik14yyml.y1x.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsABE3.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2676	powershell.exe	C:\Users\admin\AppData\Local\Temp\fjfyxf3h.tn4.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2540	powershell.exe	C:\Users\admin\AppData\Local\Temp\qedlccmr.y5l.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3572	powershell.exe	C:\Users\admin\AppData\Local\Temp\axzfeati.reo.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3816	powershell.exe	C:\Users\admin\AppData\Local\Temp\s2k4fplv.oao.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3572	powershell.exe	C:\Users\admin\AppData\Local\Temp\fjgqfftf.ztt.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2384	powershell.exe	C:\Users\admin\AppData\Local\Temp\atq5aqaf.wg2.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3816	powershell.exe	C:\Users\admin\AppData\Local\Temp\2amxy5yz.kf1.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2540	powershell.exe	C:\Users\admin\AppData\Local\Temp\ynrwv1bh.n4k.psm1	binary

		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2848	powershell.exe	C:\Users\admin\AppData\Local\Temp\spxwuskw.pa0.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2848	powershell.exe	C:\Users\admin\AppData\Local\Temp\ls0qybql.p3p.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB10C.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAFC1.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAD2D.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsAE77.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
416	powershell.exe	C:\Users\admin\AppData\Local\Temp\r5fmjzgs.ptl.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
980	powershell.exe	C:\Users\admin\AppData\Local\Temp\f4vcwdge.wwp.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
980	powershell.exe	C:\Users\admin\AppData\Local\Temp\cno32gz4.pvc.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB40D.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
416	powershell.exe	C:\Users\admin\AppData\Local\Temp\gyayvqzz.dmh.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2592	powershell.exe	C:\Users\admin\AppData\Local\Temp\th0gtnr4.fwx.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3696	powershell.exe	C:\Users\admin\AppData\Local\Temp\ksvro5e5.yvx.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2384	powershell.exe	C:\Users\admin\AppData\Local\Temp\uh21nfjs.11q.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB557.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3696	powershell.exe	C:\Users\admin\AppData\Local\Temp\h1ikrlef.e1q.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB6A1.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2592	powershell.exe	C:\Users\admin\AppData\Local\Temp\hewx4k1r.hup.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB7EC.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1988	powershell.exe	C:\Users\admin\AppData\Local\Temp\0mpd2itw.u53.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1988	powershell.exe	C:\Users\admin\AppData\Local\Temp\ptq22og5.x11.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB256.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsB9A3.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
464	powershell.exe	C:\Users\admin\AppData\Local\Temp\hfjmg4kg.uwq.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
464	powershell.exe	C:\Users\admin\AppData\Local\Temp\ween3oti.l0a.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1116	powershell.exe	C:\Users\admin\AppData\Local\Temp\dmrbne05.xyg.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1116	powershell.exe	C:\Users\admin\AppData\Local\Temp\upt2gg23.otv.psm1	binary

		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2132	powershell.exe	C:\Users\admin\AppData\Local\Temp\ogquq1rm.amr.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1468	powershell.exe	C:\Users\admin\AppData\Local\Temp\rstr2z1d.tit.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC083.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBF39.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3028	powershell.exe	C:\Users\admin\AppData\Local\Temp\xe33vh5w.4ws.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2904	powershell.exe	C:\Users\admin\AppData\Local\Temp\4jewaspw.2ul.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2132	powershell.exe	C:\Users\admin\AppData\Local\Temp\g5qneefc.t4z.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBB5B.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBDEF.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1468	powershell.exe	C:\Users\admin\AppData\Local\Temp\2gl4eley.zu5.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3028	powershell.exe	C:\Users\admin\AppData\Local\Temp\4qli3uak.r25.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsBCA5.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC1CD.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2904	powershell.exe	C:\Users\admin\AppData\Local\Temp\djg4mtbb.54e.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2352	powershell.exe	C:\Users\admin\AppData\Local\Temp\2ixvkvfi.des.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2352	powershell.exe	C:\Users\admin\AppData\Local\Temp\hihdaulx.gc2.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3052	powershell.exe	C:\Users\admin\AppData\Local\Temp\afbze2tc.pei.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2692	powershell.exe	C:\Users\admin\AppData\Local\Temp\3tpaur5l.ots.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3052	powershell.exe	C:\Users\admin\AppData\Local\Temp\gf2vkcui.vo4.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2692	powershell.exe	C:\Users\admin\AppData\Local\Temp\ow0jadmw.3mx.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC317.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC9F7.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2756	powershell.exe	C:\Users\admin\AppData\Local\Temp\g2mj53s4.kpt.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1572	powershell.exe	C:\Users\admin\AppData\Local\Temp\hrxqge1n.2xm.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3248	powershell.exe	C:\Users\admin\AppData\Local\Temp\wtmpdwhk.gwv.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC6F6.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC461.tmp	executable

		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3212	powershell.exe	C:\Users\admin\AppData\Local\Temp\xvfjkxgo.skw.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC840.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3212	powershell.exe	C:\Users\admin\AppData\Local\Temp\m1cepirh.0g4.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsC5AC.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1572	powershell.exe	C:\Users\admin\AppData\Local\Temp\xe01k0wn.5tv.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2756	powershell.exe	C:\Users\admin\AppData\Local\Temp\3gg5n1og.o31.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3248	powershell.exe	C:\Users\admin\AppData\Local\Temp\teykci5i.xgs.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCB41.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2472	powershell.exe	C:\Users\admin\AppData\Local\Temp\q2cyss0g.hbt.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD06A.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3416	powershell.exe	C:\Users\admin\AppData\Local\Temp\2sdrixy0.otm.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCDD6.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2072	powershell.exe	C:\Users\admin\AppData\Local\Temp\qsu3wpxu.rsu.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD36C.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1144	powershell.exe	C:\Users\admin\AppData\Local\Temp\lewegoli.mam.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2472	powershell.exe	C:\Users\admin\AppData\Local\Temp\42fdrzoo.nyn.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3868	powershell.exe	C:\Users\admin\AppData\Local\Temp\w5isaztv.awu.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1144	powershell.exe	C:\Users\admin\AppData\Local\Temp\b5f4izug.r3a.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCC8C.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsCF20.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2072	powershell.exe	C:\Users\admin\AppData\Local\Temp\53mf3j4h.fzk.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD221.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3868	powershell.exe	C:\Users\admin\AppData\Local\Temp\e04o44p5.psy.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4016	powershell.exe	C:\Users\admin\AppData\Local\Temp\mqavvsos.o0x.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4016	powershell.exe	C:\Users\admin\AppData\Local\Temp\i4quf1wn.ner.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3416	powershell.exe	C:\Users\admin\AppData\Local\Temp\jrxg2ew5.t4w.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2432	powershell.exe	C:\Users\admin\AppData\Local\Temp\pegt25rc.dbk.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

2432	powershell.exe	C:\Users\admin\AppData\Local\Temp\vbgxeg21.4xj.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD4B6.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2120	powershell.exe	C:\Users\admin\AppData\Local\Temp\cnujcxkv.bly.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2120	powershell.exe	C:\Users\admin\AppData\Local\Temp\fxqsew5t.2of.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD600.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
1180	powershell.exe	C:\Users\admin\AppData\Local\Temp\0descpxy.5l1.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1180	powershell.exe	C:\Users\admin\AppData\Local\Temp\5z2uzma3.xp3.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1360	powershell.exe	C:\Users\admin\AppData\Local\Temp\si5fkzdp.kpa.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1076	powershell.exe	C:\Users\admin\AppData\Local\Temp\fw0bpikm.z0h.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDB28.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2096	powershell.exe	C:\Users\admin\AppData\Local\Temp\enpldzvf.rgu.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2096	powershell.exe	C:\Users\admin\AppData\Local\Temp\ckbwaz23.ncf.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD9DE.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD894.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
1360	powershell.exe	C:\Users\admin\AppData\Local\Temp\5bnkhpjq.y3h.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
276	powershell.exe	C:\Users\admin\AppData\Local\Temp\b1lye41y.3q4.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
1076	powershell.exe	C:\Users\admin\AppData\Local\Temp\2gimne0a.z1o.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
276	powershell.exe	C:\Users\admin\AppData\Local\Temp\xy2vgieg.ydm.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsD74A.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2304	powershell.exe	C:\Users\admin\AppData\Local\Temp\wphzxweu.ynd.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDC72.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2304	powershell.exe	C:\Users\admin\AppData\Local\Temp\kayndzxr.kvk.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2756	powershell.exe	C:\Users\admin\AppData\Local\Temp\sbzydngc.hzk.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDDBD.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable
2756	powershell.exe	C:\Users\admin\AppData\Local\Temp\eijmwgci.knm.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3308	powershell.exe	C:\Users\admin\AppData\Local\Temp\bdrgys0w.35h.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsDF07.tmp **MD5:** C5B9FE538654A5A259CF64C2455C5426 **SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7	executable

2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE051.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3308	powershell.exe	C:\Users\admin\AppData\Local\Temp\d3vqom5b.5l5.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1448	powershell.exe	C:\Users\admin\AppData\Local\Temp\ctnki1iw.5mw.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1448	powershell.exe	C:\Users\admin\AppData\Local\Temp\ekruxieg.4nb.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3428	powershell.exe	C:\Users\admin\AppData\Local\Temp\4brhadd5.3in.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE19B.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3428	powershell.exe	C:\Users\admin\AppData\Local\Temp\4as4uwfu.pj1.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2928	powershell.exe	C:\Users\admin\AppData\Local\Temp\dajfdags.p5e.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE2E5.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2928	powershell.exe	C:\Users\admin\AppData\Local\Temp\pluafx0m.u42.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2848	powershell.exe	C:\Users\admin\AppData\Local\Temp\pseffrlt.tea.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE49D.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2848	powershell.exe	C:\Users\admin\AppData\Local\Temp\f1tumgf3.g1n.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE5E7.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2208	powershell.exe	C:\Users\admin\AppData\Local\Temp\gobgced5.42r.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2208	powershell.exe	C:\Users\admin\AppData\Local\Temp\xde0ftlh.c5c.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE731.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2108	powershell.exe	C:\Users\admin\AppData\Local\Temp\s5fjrclh.wjx.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2108	powershell.exe	C:\Users\admin\AppData\Local\Temp\vkbcbl3a.k0w.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3508	powershell.exe	C:\Users\admin\AppData\Local\Temp\ekj153gq.kzp.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsE87B.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2652	powershell.exe	C:\Users\admin\AppData\Local\Temp\qzwi2a3u.d10.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3508	powershell.exe	C:\Users\admin\AppData\Local\Temp\x5gcbhel.fz1.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2652	powershell.exe	C:\Users\admin\AppData\Local\Temp\dvz0n45t.hbs.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEA32.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEBEA.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1644	powershell.exe	C:\Users\admin\AppData\Local\Temp\1m4rpd0c.icl.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1644	powershell.exe	C:\Users\admin\AppData\Local\Temp\jno3toyz.edw.psm1	binary

		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsED34.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
1840	powershell.exe	C:\Users\admin\AppData\Local\Temp\rmy2aqiz.t2h.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1840	powershell.exe	C:\Users\admin\AppData\Local\Temp\2yozqeob.tfq.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
284	powershell.exe	C:\Users\admin\AppData\Local\Temp\hrd3axge.wug.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEE7E.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
284	powershell.exe	C:\Users\admin\AppData\Local\Temp\5njwdift.05q.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2388	powershell.exe	C:\Users\admin\AppData\Local\Temp\uypifx4g.x3i.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsEFC8.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2388	powershell.exe	C:\Users\admin\AppData\Local\Temp\qv0nwu1t.tam.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
4024	powershell.exe	C:\Users\admin\AppData\Local\Temp\mxdbot0a.4ko.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF112.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
4024	powershell.exe	C:\Users\admin\AppData\Local\Temp\quavyhyu.q50.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
356	powershell.exe	C:\Users\admin\AppData\Local\Temp\o1fsgchu.eyt.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
356	powershell.exe	C:\Users\admin\AppData\Local\Temp\y33xwgmc.ghf.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3140	powershell.exe	C:\Users\admin\AppData\Local\Temp\gtsn1k4e.sco.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3140	powershell.exe	C:\Users\admin\AppData\Local\Temp\3a2bxgaw.gd1.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF25D.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF3A7.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF4F1.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3960	powershell.exe	C:\Users\admin\AppData\Local\Temp\tgxqwhsr.epw.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF6A8.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3960	powershell.exe	C:\Users\admin\AppData\Local\Temp\1mgim4t1.zim.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1196	powershell.exe	C:\Users\admin\AppData\Local\Temp\rbpguwou.cjy.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1196	powershell.exe	C:\Users\admin\AppData\Local\Temp\wmeifyku.ctf.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
2628	ხელშეკრულების დოკუმენტი.exe	C:\Users\admin\AppData\Local\Temp\nsv60F5.tmp\nsF860.tmp	executable
		MD5: C5B9FE538654A5A259CF64C2455C5426	**SHA256:** 7B51372117960E84D6F5EB3A26810CC044FF02283B3D656A0A456B0AB5CB8EA7
3996	powershell.exe	C:\Users\admin\AppData\Local\Temp\pk0qhx35.akv.ps1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
3996	powershell.exe	C:\Users\admin\AppData\Local\Temp\qs2tu0iw.hof.psm1	binary
		MD5: C4CA4238A0B923820DCC509A6F75849B	**SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

Network activity

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

HTTP requests

No HTTP requests

Connections

No data

DNS requests

No data

Threats

No threats detected

Debug output strings

No debug info