



General Info

| | |
|----------------|---|
| File name: | MAYBANK BEHAD.exe |
| Full analysis: | https://app.any.run/tasks/0954ff8d-b98b-4537-92ac-878b9e87ecad |
| Verdict: | Malicious activity |
| Threats: | Agent Tesla |
| | Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold. |
| Analysis date: | August 20, 2022 at 19:47:11 |
| OS: | Windows 7 Professional Service Pack 1 (build: 7601, 32 bit) |
| Tags: | agenttesla |
| Indicators: | |
| MIME: | application/x-dosexec |
| File info: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| MD5: | E35FC8E11556F2B2AA53BAC3DF39F1B6 |
| SHA1: | 4A49ECE8B0E7CB464598430C687DD9312D0876E4 |
| SHA256: | 79CF42C43EE93818EDDBB4DFD7E0ABEA7C856FB4B7BC789CBD6F57BD34819C2E |
| SSDEEP: | 12288:kuQyxclHqGCOX02ud9x8oAW57vmC3GhNlIO64mgiQitDm0:kuQfsviHx8o357rWQIKLh |

Software environment set and analysis options

Launch configuration

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

Software preset

Internet Explorer 11.0.9600.19596 KB4534251

Adobe Acrobat Reader DC (20.013.20064)

Adobe Flash Player 32 ActiveX (32.0.0.453)

Adobe Flash Player 32 NPAPI (32.0.0.453)

Adobe Flash Player 32 PPAPI (32.0.0.453)

Adobe Refresh Manager (1.8.0)

CCleaner (5.74)

FileZilla Client 3.51.0 (3.51.0)

Google Chrome (86.0.4240.198)

Google Update Helper (1.3.36.31)

Java 8 Update 271 (8.0.2710.9)

Java Auto Updater (2.8.271.9)

Microsoft .NET Framework 4.5.2 (4.5.51209)

Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)

Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)

Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)

Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)

Hotfixes

Client LanguagePack Package

Client Refresh LanguagePack Package

CodecPack Basic Package

Foundation Package

IE Hyphenation Parent Package English

IE Spelling Parent Package English

IE Troubleshooters Package

InternetExplorer Optional Package

InternetExplorer Package TopLevel

KB2479943

KB2491683

KB2506212

KB2506928

KB2532531

KB2533552

KB2533623

KB2534111

KB2545698

KB2547666

KB2552343

KB2560656

KB2564958

KB2574819

KB2579686

KB2585542

KB2604115

KB2620704

KB2621440

KB2631813

KB2639308

KB2640148

KB2653956

KB2654428

KB2656356

KB2660075

KB2667402

KB2676562

KB2685811

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

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

| | |
|--|--|
| Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219) | KB3156016 |
| Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0) | KB3159398 |
| Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005) | KB3161102 |
| Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005) | KB3161949 |
| Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2) | KB3170735 |
| Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702) | KB3172605 |
| Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702) | KB3179573 |
| Mozilla Firefox 83.0 (x86 en-US) (83.0) | KB3184143 |
| Mozilla Maintenance Service (83.0.0.7621) | KB3185319 |
| Notepad++ (32-bit x86) (7.9.1) | KB4019990 |
| Opera 12.15 (12.15.1748) | KB4040980 |
| QGA (2.14.33) | KB4474419 |
| Skype version 8.29 (8.29) | KB4490628 |
| VLC media player (3.0.11) | KB4524752 |
| WinRAR 5.91 (32-bit) (5.91.0) | KB4532945 |
| | KB4536952 |
| | KB4567409 |
| | KB958488 |
| | KB976902 |
| | KB982018 |
| | LocalPack AU Package |
| | LocalPack CA Package |
| | LocalPack GB Package |
| | LocalPack US Package |
| | LocalPack ZA Package |
| | Package 21 for KB2984976 |
| | Package 38 for KB2984976 |
| | Package 45 for KB2984976 |
| | Package 59 for KB2984976 |
| | Package 7 for KB2984976 |
| | Package 76 for KB2984976 |
| | PlatformUpdate Win7 SRV08R2 Package TopLevel |
| | ProfessionalEdition |
| | RDP BlueIP Package TopLevel |
| | RDP WinIP Package TopLevel |
| | RollupFix |
| | UltimateEdition |
| | WUClient SelfUpdate ActiveX |
| | WUClient SelfUpdate Aux TopLevel |
| | WUClient SelfUpdate Core TopLevel |
| | WinMan WinIP Package TopLevel |

Behavior activities

| MALICIOUS | SUSPICIOUS | INFO |
|--|---|--|
| <p>Drops executable file immediately after starts MAYBANK BEHAD.exe (PID: 3332)</p> <p>Steals credentials from Web Browsers MAYBANK BEHAD.exe (PID: 2520)</p> <p>Actions looks like stealing of personal data MAYBANK BEHAD.exe (PID: 2520)</p> <p>AGENTTESLA detected by memory dumps MAYBANK BEHAD.exe (PID: 2520)</p> | <p>Reads the computer name MAYBANK BEHAD.exe (PID: 3332) MAYBANK BEHAD.exe (PID: 2520)</p> <p>Checks supported languages MAYBANK BEHAD.exe (PID: 3332) MAYBANK BEHAD.exe (PID: 2520)</p> <p>Executable content was dropped or overwritten MAYBANK BEHAD.exe (PID: 3332)</p> <p>Drops a file with a compile date too recent MAYBANK BEHAD.exe (PID: 3332)</p> <p>Reads Environment values MAYBANK BEHAD.exe (PID: 2520)</p> <p>Application launched itself MAYBANK BEHAD.exe (PID: 3332)</p> | <p>Checks supported languages schtasks.exe (PID: 3424)</p> <p>Reads settings of System Certificates MAYBANK BEHAD.exe (PID: 2520)</p> <p>Reads the computer name schtasks.exe (PID: 3424)</p> |

Static information

| TRiD | EXIF |
|---|--|
| <p>.exe Generic CIL Executable (.NET, Mono, etc.) (82.9)</p> <p>.dll Win32 Dynamic Link Library (generic) (7.4)</p> <p>.exe Win32 Executable (generic) (5.1)</p> <p>.exe Generic Win/DOS Executable (2.2)</p> | <p>EXE</p> <p>MachineType: Intel 386 or later, and compatibles</p> <p>TimeStamp: 2022:08:19 16:04:59+02:00</p> <p>PEType: PE32</p> |

| | | | |
|-------------------------------------|--|------------------------|------------------------|
| .exe DOS Executable Generic (2.2) | | LinkerVersion: | 80 |
| | | CodeSize: | 512000 |
| | | InitializedDataSize: | 97280 |
| | | UninitializedDataSize: | 0 |
| | | EntryPoint: | 0x7eea6 |
| | | OSVersion: | 4 |
| | | ImageVersion: | 0 |
| | | SubsystemVersion: | 4 |
| | | Subsystem: | Windows GUI |
| | | FileVersionNumber: | 1.0.0.0 |
| | | ProductVersionNumber: | 1.0.0.0 |
| | | FileFlagsMask: | 0x003f |
| | | FileFlags: | (none) |
| | | FileOS: | Win32 |
| | | ObjectFileType: | Executable application |
| | | FileSubtype: | 0 |
| | | LanguageCode: | Neutral |
| | | CharacterSet: | Unicode |
| | | Comments: | |
| | | CompanyName: | Microsoft Corporation |
| | | FileDescription: | Multi ComboBox |
| | | FileVersion: | 1.0.0.0 |
| | | InternalName: | xlea4.exe |
| | | LegalCopyright: | Copyright © 2019 |
| | | LegalTrademarks: | |
| | | OriginalFileName: | xlea4.exe |
| | | ProductName: | Multi ComboBox |
| | | ProductVersion: | 1.0.0.0 |
| | | AssemblyVersion: | 1.0.0.0 |

Summary

| | |
|-------------------|-----------------------------|
| Architecture: | IMAGE_FILE_MACHINE_I386 |
| Subsystem: | IMAGE_SUBSYSTEM_WINDOWS_GUI |
| Compilation Date: | 19-Aug-2022 14:04:59 |
| Comments: | |
| CompanyName: | Microsoft Corporation |
| FileDescription: | Multi ComboBox |
| FileVersion: | 1.0.0.0 |
| InternalName: | xlea4.exe |
| LegalCopyright: | Copyright © 2019 |
| LegalTrademarks: | |
| OriginalFilename: | xlea4.exe |
| ProductName: | Multi ComboBox |
| ProductVersion: | 1.0.0.0 |
| Assembly Version: | 1.0.0.0 |

DOS Header

| | |
|-----------------------------|------------|
| Magic number: | MZ |
| Bytes on last page of file: | 0x0090 |
| Pages in file: | 0x0003 |
| 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: | 0x00000080 |

PE Headers

| | |
|--------------------------|---|
| Signature: | PE |
| Machine: | IMAGE_FILE_MACHINE_I386 |
| Number of sections: | 3 |
| Time date stamp: | 19-Aug-2022 14:04:59 |
| Pointer to Symbol Table: | 0x00000000 |
| Number of symbols: | 0 |
| Size of Optional Header: | 0x00E0 |
| Characteristics: | IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE |

Sections

| Name | Virtual Address | Virtual Size | Raw Size | Charateristics | Entropy |
|-------|-----------------|--------------|------------|---|---------|
| .text | 0x00002000 | 0x0007CEAC | 0x0007D000 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ | 7.45312 |

| | | | | | |
|--------|------------|------------|------------|---|---------|
| .src | 0x00080000 | 0x000179BC | 0x00017A00 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ | 2.8764 |
| .reloc | 0x00098000 | 0x0000000C | 0x00000200 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ | 0.10191 |

Resources

| Title | Entropy | Size | Codepage | Language | Type |
|-------|---------|------|----------------------------|----------|-------------|
| 1 | 5.00112 | 490 | Latin 1 / Western European | UNKNOWN | RT_MANIFEST |

Imports

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

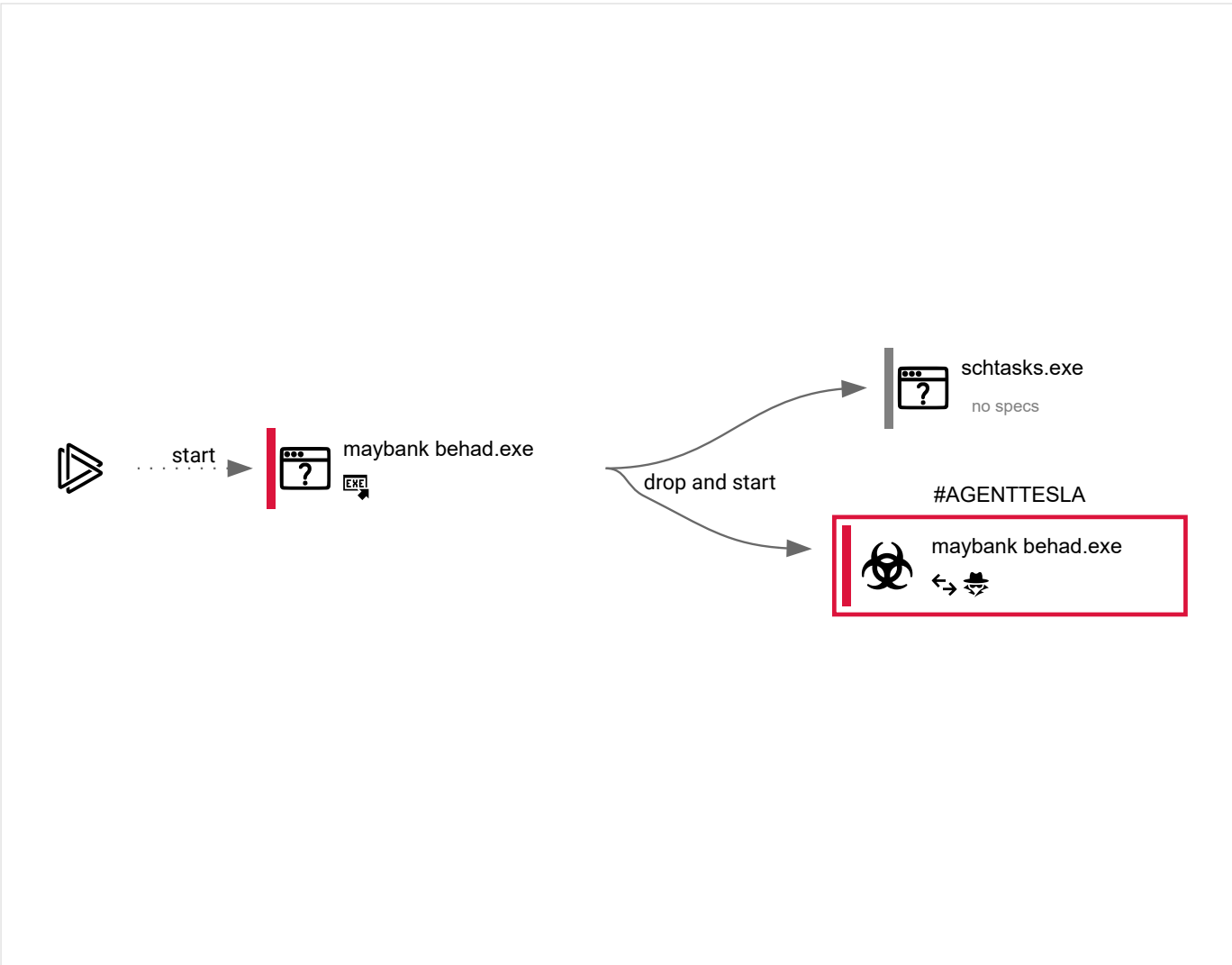
Video and screenshots



Processes

| | | | |
|-----------------|---------------------|---------------------|----------------------|
| Total processes | Monitored processes | Malicious processes | Suspicious processes |
| 38 | 3 | 2 | 0 |

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 | | | | | | | | | | | | | | | |
|--|---|---|-----------------------|----------------|-------|-------|----------|-----------------------|--|------------------|--------|--------------|----------------|--|------------|---|----------|---------|--|
| 3332 | "C:\Users\admin\AppData\Local\Temp\MAYBANK BEHAD.exe" | C:\Users\admin\AppData\Local\Temp\MAYBANK BEHAD.exe | | Explorer.EXE | | | | | | | | | | | | | | | |
| <div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Microsoft Corporation</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">Multi ComboBox</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">1.0.0.0</td></tr></table> | | | | | User: | admin | Company: | Microsoft Corporation | | Integrity Level: | MEDIUM | Description: | Multi ComboBox | | Exit code: | 0 | Version: | 1.0.0.0 | |
| User: | admin | Company: | Microsoft Corporation | | | | | | | | | | | | | | | | |
| Integrity Level: | MEDIUM | Description: | Multi ComboBox | | | | | | | | | | | | | | | | |
| Exit code: | 0 | Version: | 1.0.0.0 | | | | | | | | | | | | | | | | |

3424

"C:\Windows\System32\schtasks.exe" /Create /TN
"Updates\WRCqmia" /XML
"C:\Users\admin\AppData\Local\Temp\tmpEC16.tmp"

C:\Windows\System32\schtasks.exe

—

MAYBANK BEHAD.exe

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Manages scheduled tasks

Exit code:

0




Version:

6.1.7600.16385 (win7_rtm.090713-1255)

2520

"(path)"

C:\Users\admin\AppData\Local\Temp\MAYBANK BEHAD.exe

MAYBANK BEHAD.exe

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Multi ComboBox

Version:

1.0.0.0

Registry activity

| | | | |
|--------------|-------------|--------------|---------------|
| Total events | Read events | Write events | Delete events |
| 4 840 | 4 818 | 22 | 0 |

Modification events

| | | | |
|----------------|--------------------------|-------|---|
| (PID) Process: | (3332) MAYBANK BEHAD.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation: | write | Name: | ProxyBypass |
| Value: | 1 | | |

| | | | |
|----------------|--------------------------|-------|---|
| (PID) Process: | (3332) MAYBANK BEHAD.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation: | write | Name: | IntranetName |
| Value: | 1 | | |

| | | | |
|----------------|--------------------------|-------|---|
| (PID) Process: | (3332) MAYBANK BEHAD.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation: | write | Name: | UNCAsIntranet |
| Value: | 1 | | |

| | | | |
|----------------|--------------------------|-------|---|
| (PID) Process: | (3332) MAYBANK BEHAD.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation: | write | Name: | AutoDetect |
| Value: | 0 | | |

| | | | |
|----------------|--------------------------|-------|--|
| (PID) Process: | (2520) MAYBANK BEHAD.exe | Key: | HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C6487E |
| Operation: | write | Name: | LanguageList |
| Value: | en-US | | |

Files activity

| | | | |
|------------------|------------------|------------|---------------|
| Executable files | Suspicious files | Text files | Unknown types |
| 1 | 3 | 1 | 1 |

Dropped files

| PID | Process | Filename | Type |
|------|-------------------|---|------------|
| 2520 | MAYBANK BEHAD.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 MD5: 482C7E9B4FE0D3EAD4548010064BFDEE SHA256: 940095268DA256C31A8291007EEE4B80B71761C65AF811B52215ACCODE4548BF | binary |
| 3332 | MAYBANK BEHAD.exe | C:\Users\admin\AppData\Local\Temp\tmpEC16.tmp MD5: 7B98D536D3837EE614C407950C7AF62E SHA256: A10A27E7785C08703AEBBEADF0DABE75EB7840E9D278EA81A222572D0AE779D4 | xml |
| 2520 | MAYBANK BEHAD.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 MD5: 589C442FC7A0C70DCA927115A700D41E SHA256: 2E5CB72E9EB43BAAF6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A | compressed |
| 3332 | MAYBANK BEHAD.exe | C:\Users\admin\AppData\Roaming\WRCqmia.exe MD5: E35FC8E11556F2B2AA53BAC3DF39F1B6 SHA256: 79CF42C43EE93818EDDBB4DFD7E0ABEA7C856FB4B7BC789CBD6F57BD34819C2E | executable |
| 2520 | MAYBANK BEHAD.exe | C:\Users\admin\AppData\Local\Temp\Tar1B2.tmp MD5: 7EE994C83F2744D702CBA18693ED1758 SHA256: 5DB917AB6DC8A42A43617850DFBE2C7F26A7F810B229B349E9DD2A2D615671D2 | cat |
| 2520 | MAYBANK BEHAD.exe | C:\Users\admin\AppData\Local\Temp\Cab1B1.tmp MD5: 589C442FC7A0C70DCA927115A700D41E SHA256: 2E5CB72E9EB43BAAF6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A | compressed |

Network activity

| | | | |
|------------------|---------------------|--------------|---------|
| HTTP(S) requests | TCP/UDP connections | DNS requests | Threats |
| 1 | 2 | 2 | 1 |

HTTP requests

| PID | Process | Method | HTTP Code | IP | URL | CN | Type | Size | Reputation |
|------|-------------------|--------|-----------|-------------------|---|----|------------|---------|-------------|
| 2520 | MAYBANK BEHAD.exe | GET | 200 | 93.184.221.240:80 | http://ctldl.windowsupdate.com/msdownload/update/v3/stati c/trustedr/en/authrootstl.cab?92b36f355c7b8f14 | US | compressed | 60.2 Kb | whitelisted |

Connections

| PID | Process | IP | Domain | ASN | CN | Reputation |
|------|-------------------|---------------------|-------------------------|---|----|-------------|
| 2520 | MAYBANK BEHAD.exe | 162.222.225.250:587 | mail.dinrack.com | PDR | US | malicious |
| 2520 | MAYBANK BEHAD.exe | 93.184.221.240:80 | ctldl.windowsupdate.com | MCI Communications Services, Inc. d/b/a Verizon Business | US | whitelisted |

DNS requests

| Domain | IP | Reputation |
|-------------------------|-----------------|-------------|
| mail.dinrack.com | 162.222.225.250 | unknown |
| ctldl.windowsupdate.com | 93.184.221.240 | whitelisted |

Threats

| PID | Process | Class | Message |
|------|-------------------|---------------------------------|--|
| 2520 | MAYBANK BEHAD.exe | Generic Protocol Command Decode | SURICATA Applayer Detect protocol only one direction |

Debug output strings

No debug info



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