ANY ▷ RUN
INTERACTIVE MALWARE ANALYSIS

# General Info

| | |
|---|---|
| File name: | MURATA PURCHASE ORDER,pdf.exe |
| Full analysis: | https://app.any.run/tasks/5e3fac41-2f54-4fe3-83b2-963ff56cbc23 |
| Verdict: | Malicious activity |
| Threats: | **Remcos** |
| | Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month. |
| Analysis date: | August 17, 2022 at 16:50:04 |
| OS: | Windows 7 Professional Service Pack 1 (build: 7601, 32 bit) |
| Tags: | remcos |
| Indicators: | ☣ ⚒ ☎ 🖿 🖳 🏁 |
| MIME: | application/x-dosexec |
| File info: | PE32 executable (GUI) Intel 80386, for MS Windows |
| MD5: | 060E2BC9D5AED0B0033EC7E5E570B131 |
| SHA1: | EF05CB824D79EE9FD9E528A6DAC49BAE6276AB73 |
| SHA256: | C7C1A88E84BB85E9437B450DE1E701473081B8CF7E45DCF62FD317262BFB2970 |
| SSDEEP: | 12288:ei0wFFLy44jTpuNaCT8pT2m+lj6RSul8z7iEzwSK1CHaJFQmNL5OWZdavN2HuEGU:lHWTkNaw8pT2zMS3v9RDeB4FvzJK |

---

| 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 | Hotfixes |
|---|---|
| Internet Explorer 11.0.9600.19596 KB4534251 | Client LanguagePack Package |
| Adobe Acrobat Reader DC (20.013.20064) | Client Refresh LanguagePack Package |
| Adobe Flash Player 32 ActiveX (32.0.0.453) | CodecPack Basic Package |
| Adobe Flash Player 32 NPAPI (32.0.0.453) | Foundation Package |
| Adobe Flash Player 32 PPAPI (32.0.0.453) | IE Hyphenation Parent Package English |
| Adobe Refresh Manager (1.8.0) | IE Spelling Parent Package English |
| CCleaner (5.74) | IE Troubleshooters Package |
| FileZilla Client 3.51.0 (3.51.0) | InternetExplorer Optional Package |
| Google Chrome (86.0.4240.198) | InternetExplorer Package TopLevel |
| Google Update Helper (1.3.36.31) | KB2479943 |
| Java 8 Update 271 (8.0.2710.9) | KB2491683 |
| Java Auto Updater (2.8.271.9) | KB2506212 |
| Microsoft .NET Framework 4.5.2 (4.5.51209) | KB2506928 |
| Microsoft Office Access MUI (English) 2010 (14.0.6029.1000) | KB2532531 |
| Microsoft Office Access MUI (French) 2010 (14.0.4763.1000) | KB2533552 |
| Microsoft Office Access MUI (German) 2010 (14.0.4763.1000) | KB2533623 |
| Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000) | KB2534111 |
| Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000) | KB2545698 |
| Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000) | KB2547666 |
| Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000) | KB2552343 |
| Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000) | KB2560656 |
| Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000) | KB2564958 |
| Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013) | KB2574819 |
| Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000) | KB2579686 |
| Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000) | KB2585542 |
| Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000) | KB2604115 |
| Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000) | KB2620704 |
| Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000) | KB2621440 |
| Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000) | KB2631813 |
| Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000) | KB2639308 |
| Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000) | KB2640148 |
| Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000) | KB2653956 |
| Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000) | KB2654428 |
| Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013) | KB2656356 |
| Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000) | KB2660075 |
| Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000) | KB2667402 |
| Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000) | KB2676562 |
| Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000) | 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

**Changes the autorun value in the registry**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**Drops executable file immediately after starts**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**REMCOS detected by memory dumps**
rasphone.exe (PID: 2424)

### SUSPICIOUS

**Reads the computer name**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**Checks supported languages**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**Drops a file with a compile date too recent**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**Executable content was dropped or overwritten**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

### INFO

**Reads settings of System Certificates**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**Checks Windows Trust Settings**
MURATA PURCHASE ORDER,pdf.exe (PID: 400)

**Checks supported languages**
rasphone.exe (PID: 2424)

# Static information

## TRiD

| | | |
|---|---|---|
| .exe | | Win32 Executable Borland Delphi 7 (94.6) |
| .exe | | Win32 Executable Delphi generic (2) |
| .scr | | Windows screen saver (1.8) |
| .exe | | Win32 Executable (generic) (0.6) |
| .exe | | Win16/32 Executable Delphi generic (0.2) |

## EXIF

### EXE

| | |
|---|---|
| Subsystem: | Windows GUI |
| SubsystemVersion: | 4 |
| ImageVersion: | 0 |
| OSVersion: | 4 |
| EntryPoint: | 0x958c4 |
| UninitializedDataSize: | 0 |
| InitializedDataSize: | 384000 |
| CodeSize: | 607232 |
| LinkerVersion: | 2.25 |

| | |
|---|---|
| PEType: | PE32 |
| TimeStamp: | 1992:06:20 00:22:17+02:00 |
| MachineType: | Intel 386 or later, and compatibles |

## Summary

| | |
|---|---|
| Architecture: | IMAGE_FILE_MACHINE_I386 |
| Subsystem: | IMAGE_SUBSYSTEM_WINDOWS_GUI |
| Compilation Date: | 19-Jun-1992 22:22:17 |
| Detected languages: | English - United States |

## DOS Header

| | |
|---|---|
| Magic number: | MZ |
| Bytes on last page of file: | 0x0050 |
| Pages in file: | 0x0002 |
| Relocations: | 0x0000 |
| Size of header: | 0x0004 |
| Min extra paragraphs: | 0x000F |
| Max extra paragraphs: | 0xFFFF |
| Initial SS value: | 0x0000 |
| Initial SP value: | 0x00B8 |
| Checksum: | 0x0000 |
| Initial IP value: | 0x0000 |
| Initial CS value: | 0x0000 |
| Overlay number: | 0x001A |
| OEM identifier: | 0x0000 |
| OEM information: | 0x0000 |
| Address of NE header: | 0x00000100 |

## PE Headers

| | |
|---|---|
| Signature: | PE |
| Machine: | IMAGE_FILE_MACHINE_I386 |
| Number of sections: | 9 |
| Time date stamp: | 19-Jun-1992 22:22:17 |
| Pointer to Symbol Table: | 0x00000000 |
| Number of symbols: | 0 |
| Size of Optional Header: | 0x00E0 |
| Characteristics: | IMAGE_FILE_32BIT_MACHINE |
| | IMAGE_FILE_BYTES_REVERSED_HI |
| | IMAGE_FILE_BYTES_REVERSED_LO |
| | IMAGE_FILE_EXECUTABLE_IMAGE |
| | IMAGE_FILE_LINE_NUMS_STRIPPED |
| | IMAGE_FILE_LOCAL_SYMS_STRIPPED |

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Charateristics | Entropy |
|---|---|---|---|---|---|
| .text | 0x00001000 | 0x00093954 | 0x00093A00 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ | 6.56864 |
| .itext | 0x00095000 | 0x0000090C | 0x00000A00 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ | 5.90976 |
| .data | 0x00096000 | 0x000028FC | 0x00002A00 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE | 4.39912 |
| .bss | 0x00099000 | 0x0000388C | 0x00000000 | IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE | 0 |
| .idata | 0x0009D000 | 0x00002AC6 | 0x00002C00 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE | 5.13086 |
| .tls | 0x000A0000 | 0x00000040 | 0x00000000 | IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE | 0 |
| .rdata | 0x000A1000 | 0x00000018 | 0x00000200 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ | 0.170146 |
| .reloc | 0x000A2000 | 0x00009100 | 0x00009200 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ | 6.66039 |
| .rsrc | 0x000AC000 | 0x0004F1B8 | 0x0004F200 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ | 6.22049 |

## Resources

| Title | Entropy | Size | Codepage | Language | Type |
|---|---|---|---|---|---|
| 65 | 2.23329 | 16936 | UNKNOWN | UNKNOWN | RT_ICON |
| 66 | 2.22424 | 14920 | UNKNOWN | UNKNOWN | RT_ICON |
| 71 | 3.09784 | 1720 | UNKNOWN | UNKNOWN | RT_ICON |
| 72 | 3.10512 | 1128 | UNKNOWN | UNKNOWN | RT_ICON |
| 4081 | 2.9322 | 328 | UNKNOWN | UNKNOWN | RT_STRING |
| 4082 | 3.45914 | 936 | UNKNOWN | UNKNOWN | RT_STRING |
| 4083 | 3.27638 | 1224 | UNKNOWN | UNKNOWN | RT_STRING |
| 4084 | 3.44967 | 156 | UNKNOWN | UNKNOWN | RT_STRING |
| 4085 | 3.3924 | 236 | UNKNOWN | UNKNOWN | RT_STRING |
| 4086 | 3.3624 | 408 | UNKNOWN | UNKNOWN | RT_STRING |
| 4087 | 3.30108 | 1144 | UNKNOWN | UNKNOWN | RT_STRING |
| 4088 | 3.29364 | 840 | UNKNOWN | UNKNOWN | RT_STRING |
| 4089 | 3.28906 | 908 | UNKNOWN | UNKNOWN | RT_STRING |
| 4090 | 3.33629 | 1016 | UNKNOWN | UNKNOWN | RT_STRING |

| 4091 | 3.2817 | 280 | UNKNOWN | UNKNOWN | RT_STRING |
|---|---|---|---|---|---|
| 4092 | 3.34426 | 204 | UNKNOWN | UNKNOWN | RT_STRING |
| 4093 | 3.38717 | 520 | UNKNOWN | UNKNOWN | RT_STRING |
| 4094 | 3.2658 | 972 | UNKNOWN | UNKNOWN | RT_STRING |
| 4095 | 3.35521 | 852 | UNKNOWN | UNKNOWN | RT_STRING |
| 4096 | 3.27314 | 676 | UNKNOWN | UNKNOWN | RT_STRING |
| BBABORT | 2.92079 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBALL | 3.16995 | 484 | UNKNOWN | English - United States | RT_BITMAP |
| BBCANCEL | 2.92079 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBCLOSE | 3.68492 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBHELP | 2.88085 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBIGNORE | 3.29718 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBNO | 3.58804 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBOK | 2.67459 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBOKK | 5.48978 | 187864 | UNKNOWN | English - United States | RT_BITMAP |
| BBRETRY | 3.53344 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| BBYES | 2.67459 | 464 | UNKNOWN | English - United States | RT_BITMAP |
| PREVIEWGLYPH | 2.85172 | 232 | UNKNOWN | English - United States | RT_BITMAP |
| ALOTRO | 4.02826 | 40774 | UNKNOWN | English - United States | RT_RCDATA |
| DVCLAL | 4 | 16 | UNKNOWN | UNKNOWN | RT_RCDATA |
| PACKAGEINFO | 5.38347 | 848 | UNKNOWN | UNKNOWN | RT_RCDATA |
| TFLIPPER | 6.59032 | 41975 | UNKNOWN | UNKNOWN | RT_RCDATA |
| MAINICON | 2.83146 | 62 | UNKNOWN | UNKNOWN | RT_GROUP_ICON |

## Imports

| |
|---|
| advapi32.dll |
| comctl32.dll |
| gdi32.dll |
| kernel32.dll |
| ole32.dll |
| oleacc.dll |
| oleaut32.dll |
| user32.dll |
| version.dll |
| winmm.dll |

# Video and screenshots
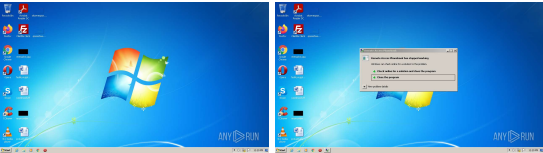
## Processes

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

## Behavior graph

start → murata purchase order,pdf.exe → #REMCOS rasphone.exe
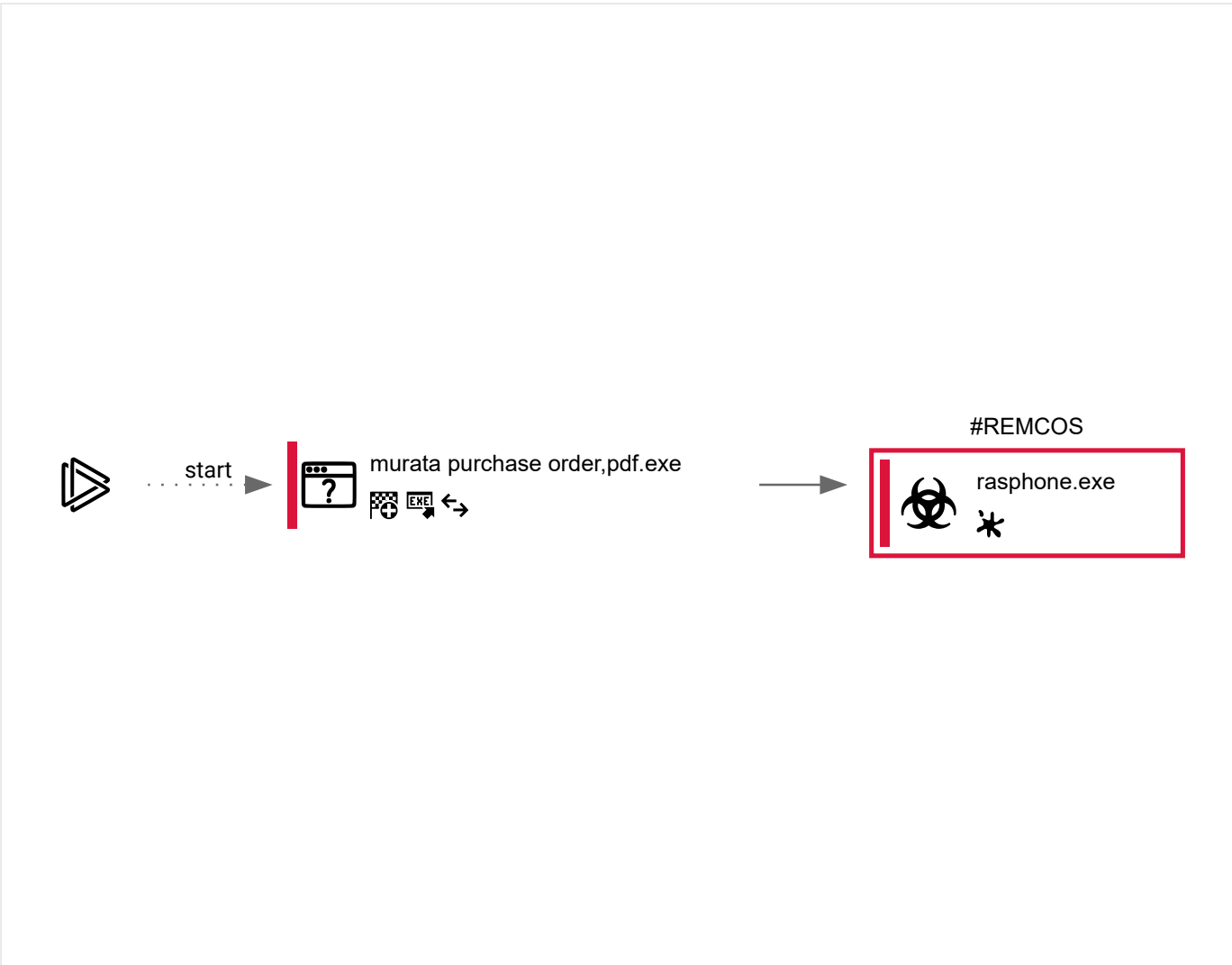
## Specs description

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 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 |
|---|---|---|---|---|
| 400 | "C:\Users\admin\AppData\Local\Temp\MURATA PURCHASE ORDER,pdf.exe" | C:\Users\admin\AppData\Local\Temp\MURATA PURCHASE ORDER,pdf.exe | | Explorer.EXE |

| Information | | | |
|---|---|---|---|
| User: | admin | Integrity Level: | MEDIUM |
| Exit code: | 0 | | |

| 2424 | "C:\Windows\System32\rasphone.exe" | | C:\Windows\System32\rasphone.exe | ⚒ ☠ ✳ | MURATA PURCHASE ORDER,pdf.exe |

| Information | | | | |
|---|---|---|---|---|
| User: | admin | Company: | Microsoft Corporation | |
| Integrity Level: | MEDIUM | Description: | Remote Access Phonebook | |
| Version: | 6.1.7600.16385 (win7_rtm.090713-1255) | | | |

## Registry activity

| Total events | Read events | Write events | Delete events |
|---|---|---|---|
| 4 443 | 4 408 | 35 | 0 |

### Modification events

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings |
|---|---|---|---|
| Operation: | write | Name: | ProxyEnable |
| Value: | 0 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections |
|---|---|---|---|
| Operation: | write | Name: | SavedLegacySettings |

Value: 460000003B010000090000000000000000000000000000000040000000000000000C0E333BBEAB1D3010000000000000000000000000001000000020000000C0A80164000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content |
|---|---|---|---|
| Operation: | write | Name: | CachePrefix |
| Value: | | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies |
|---|---|---|---|
| Operation: | write | Name: | CachePrefix |
| Value: | Cookie: | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History |
|---|---|---|---|
| Operation: | write | Name: | CachePrefix |
| Value: | Visited: | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
|---|---|---|---|
| Operation: | write | Name: | ProxyBypass |
| Value: | 1 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
|---|---|---|---|
| Operation: | write | Name: | IntranetName |
| Value: | 1 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
|---|---|---|---|
| Operation: | write | Name: | UNCAsIntranet |
| Value: | 1 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
|---|---|---|---|
| Operation: | write | Name: | AutoDetect |
| Value: | 0 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47} |
|---|---|---|---|
| Operation: | write | Name: | WpadDecisionReason |
| Value: | 1 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47} |
|---|---|---|---|
| Operation: | write | Name: | WpadDecisionTime |
| Value: | 0916B85C2BB2D801 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47} |
|---|---|---|---|
| Operation: | write | Name: | WpadDecision |
| Value: | 0 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47} |
|---|---|---|---|
| Operation: | write | Name: | WpadNetworkName |
| Value: | Network 3 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff |
|---|---|---|---|
| Operation: | write | Name: | WpadDecisionReason |
| Value: | 1 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff |
|---|---|---|---|
| Operation: | write | Name: | WpadDecisionTime |
| Value: | 0916B85C2BB2D801 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff |
|---|---|---|---|
| Operation: | write | Name: | WpadDecision |
| Value: | 0 | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E |
|---|---|---|---|
| Operation: | write | Name: | LanguageList |
| Value: | en-US | | |

| (PID) Process: | (400) MURATA PURCHASE ORDER,pdf.exe | Key: | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run |
|---|---|---|---|
| Operation: | write | Name: | Xelmeucql |
| Value: | C:\Users\Public\Libraries\lqcuemleX.url | | |

# Files activity

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

## Dropped files

| PID | Process | Filename | | Type |
|---|---|---|---|---|
| 400 | MURATA PURCHASE ORDER,pdf.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 | | compressed |
| | | MD5: F7DCB24540769805E5BB30D193944DCE | SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA | |
| 400 | MURATA PURCHASE ORDER,pdf.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 | | binary |
| | | MD5: F9C1AA103608ECD6A1CB72363EC15662 | SHA256: 6B25F4917C374EAB8F51801869F52A173A920C140D7AF120F68EAB80BEAE6724 | |
| 400 | MURATA PURCHASE ORDER,pdf.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD 387E155AD0BA27 | | binary |
| | | MD5: 4D57042064890794CC4441073E80DB5A | SHA256: 3507667E6F7BC4616E969E5F3A659342038649DBA4FBE15946ACC760DF66ACF1 | |
| 400 | MURATA PURCHASE ORDER,pdf.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD3 87E155AD0BA27 | | der |
| | | MD5: 12F3AF5F3D0561B18ECC2C6AD183C03A | SHA256: BFFE5EA2636B3EEDB9676387CDC436026DCDAB4A0C9783E9C6CCE48BCC0A11DF | |
| 400 | MURATA PURCHASE ORDER,pdf.exe | C:\Users\Public\Libraries\lqcuemleX.url | | text |
| | | MD5: 3F8488501951ECE90B9457EA356FA52F | SHA256: 2C5483759474D6B5A45B134479C235174FE62C8F6D3573811CDA207F23FC8E9B | |
| 400 | MURATA PURCHASE ORDER,pdf.exe | C:\Users\Public\Libraries\Xelmeucql.exe | | executable |
| | | MD5: 060E2BC9D5AED0B0033EC7E5E570B131 | SHA256: C7C1A88E84BB85E9437B450DE1E701473081B8CF7E45DCF62FD317262BFB2970 | |

# Network activity

| HTTP(S) requests | TCP/UDP connections | DNS requests | Threats |
|---|---|---|---|
| 2 | 5 | 3 | 3 |

## HTTP requests

| PID | Process | Method | HTTP Code | IP | URL | CN | Type | Size | Reputation |
|---|---|---|---|---|---|---|---|---|---|
| 400 | MURATA PURCHASE ORDER,pdf.exe | GET | 200 | 93.184.221.240:80 | http://ctldl.windowsupdate.com/msdownload/update/v3/static /trustedr/en/disallowedcertstl.cab?876787f2dee77c14 | US | compressed | 4.70 Kb | whitelisted |
| 400 | MURATA PURCHASE ORDER,pdf.exe | GET | 200 | 93.184.220.29:80 | http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgU ABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMy s%2BghUNoZ7OrUETfACEAo3h2ReX7SMIk79G%2B0UDDw%3D | US | der | 1.47 Kb | whitelisted |

## Connections

| PID | Process | IP | Domain | ASN | CN | Reputation |
|---|---|---|---|---|---|---|

| 400 | MURATA PURCHASE ORDER,pdf.exe | 162.159.133.233:443 | cdn.discordapp.com | Cloudflare Inc | – | shared |
| 400 | MURATA PURCHASE ORDER,pdf.exe | 93.184.220.29:80 | ocsp.digicert.com | MCI Communications Services, Inc. d/b/a Verizon Business | US | whitelisted |
| 400 | MURATA PURCHASE ORDER,pdf.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 |
|---|---|---|
| cdn.discordapp.com | 162.159.133.233<br>162.159.134.233<br>162.159.130.233<br>162.159.135.233<br>162.159.129.233 | shared |
| ctldl.windowsupdate.com | 93.184.221.240 | whitelisted |
| ocsp.digicert.com | 93.184.220.29 | whitelisted |

## Threats

| PID | Process | Class | Message |
|---|---|---|---|
| – | – | Misc activity | ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) |
| 400 | MURATA PURCHASE ORDER,pdf.exe | Misc activity | ET INFO Observed Discord Domain (discordapp .com in TLS SNI) |
| 400 | MURATA PURCHASE ORDER,pdf.exe | Misc activity | ET INFO Observed Discord Domain (discordapp .com in TLS SNI) |

# Debug output strings

No debug info

ANY ▷ RUN
INTERACTIVE MALWARE ANALYSIS

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