



## General Info

---

File name: Install\_New\_theme.bat  
Full analysis: <https://app.any.run/tasks/8b54408f-f0ed-4a5e-9210-2a9bc9a2a5ba>  
Verdict: Malicious activity  
Analysis date: November 01, 2023 at 13:20:43  
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)  
Indicators:

MIME: text/x-msdos-batch  
File info: DOS batch file, ASCII text  
MD5: BF78A0583EE16DE7CF3776C7C7AD23FC  
SHA1: 30D6CF358F8932007554E5A5EF2F3CCF83C90E8A  
SHA256: FA7FF9975DCE1FC26987F6457EE9EF5E9A9FBE4D21B68A34941343F5CB00651E  
SSDEEP: 6:hHox2jIny69y2A2ijPeanSBFDILh8JkzxmE+FZNbzi0wRn:5o4jIn5yD2imB8GuzxmEsZB+0wR

### Software environment set and analysis options

#### Launch configuration

---

Task duration: 60 seconds

Additional time used: none

Fakenet option: off

Network: on

Heavy Evasion option: off

MITM proxy: off

Route via Tor: off

Network geolocation: off

Privacy: Public submission

Autoconfirmation of UAC: on

## Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- Adobe Refresh Manager (1.8.0)
- CCleaner (6.14)
- CCleaner (6.14)
- FileZilla 3.65.0 (3.65.0)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (109.0.5414.120)
- Google Chrome (109.0.5414.120)
- Google Update Helper (1.3.36.31)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Edge (109.0.1518.115)
- Microsoft Edge (109.0.1518.115)
- Microsoft Edge Update (1.3.175.29)
- Microsoft Edge Update (1.3.175.29)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- 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 (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)

## Hotfixes

- Microsoft Office Excel MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 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)
- Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Korean) 2010 (14.0.4763.1000)
- Microsoft Office IME (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)
- Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)
- Microsoft Office O MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (German) 2010 (14.0.4763.1000)

- Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)

- Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)
- Microsoft Office Proof (English) 2010 (14.0.6029.1000)
- Microsoft Office Proof (English) 2010 (14.0.6029.1000)
- Microsoft Office Proof (French) 2010 (14.0.6029.1000)
- Microsoft Office Proof (French) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)
- Microsoft Office Proof (German) 2010 (14.0.4763.1000)
- Microsoft Office Proof (German) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (German) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (German) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)

- Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Single Image 2010 (14.0.6029.1000)
- Microsoft Office Single Image 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)

- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x86 en-US) (115.0.2)
- Mozilla Firefox (x86 en-US) (115.0.2)
- Mozilla Maintenance Service (115.0.2)
- Mozilla Maintenance Service (115.0.2)
- Notepad++ (32-bit x86) (7.9.1)
- Notepad++ (32-bit x86) (7.9.1)
- PowerShell 7-x86 (7.2.11.0)
- PowerShell 7-x86 (7.2.11.0)
- Skype version 8.100 (8.100)
- Skype version 8.100 (8.100)
- VLC media player (3.0.11)
- VLC media player (3.0.11)
- WinRAR 5.91 (32-bit) (5.91.0)
- WinRAR 5.91 (32-bit) (5.91.0)

## Behavior activities

### MALICIOUS

No malicious indicators.

### SUSPICIOUS

**The process executes Powershell scripts**

- cmd.exe (PID: 3572)

**Request a resource from the Internet using PowerShell's cmdlet**

- cmd.exe (PID: 3572)

**Starts POWERSHELL.EXE for commands execution**

- cmd.exe (PID: 3572)

**Powershell version downgrade attack**

- powershell.exe (PID: 2268)

**Possibly malicious use of IEX has been detected**

- cmd.exe (PID: 3572)

### INFO

No info indicators.

## Malware configuration

---

No Malware configuration.

## Static information

---

No data.

## Video and screenshots

---

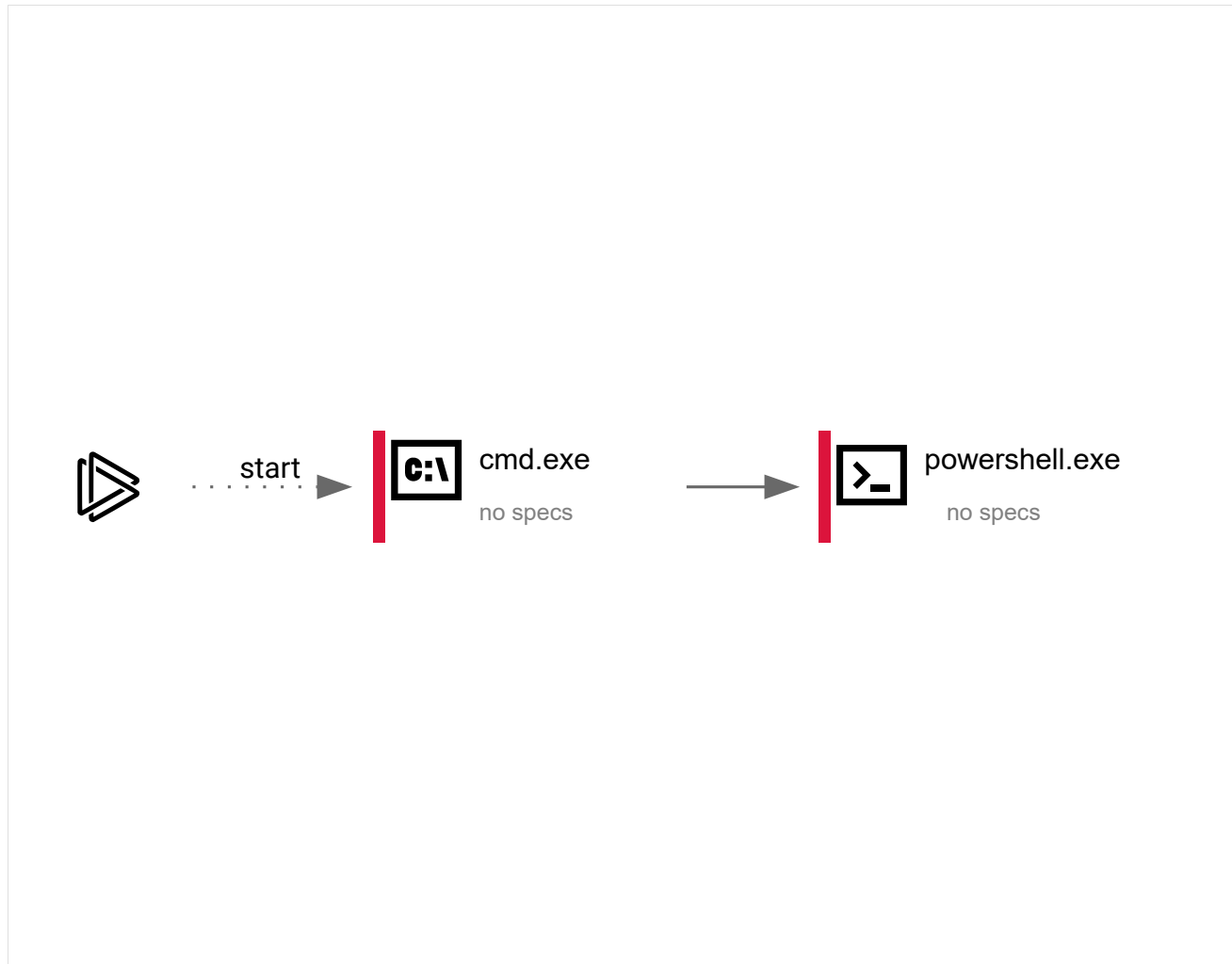




## Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	2	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
3572	C:\Windows\system32\cmd.exe /c "C:\Users\admin\Downloads\Install_New_theme.bat"	C:\Windows\System32\cmd.exe	-	explorer.exe
<b>Information</b>				
User:	admin	Company:	Microsoft Corporation	

PID	CMD	Path	Indicators	Parent process
<b>Integrity Level:</b> MEDIUM <b>Description:</b> Windows Command Processor <b>Exit code:</b> 0 <b>Version:</b> 6.1.7601.17514 (win7sp1_rtm.101119-1850)				
2268	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command "&{[Net.ServicePointManager]::SecurityProtocol = 3072}; "" & { \$(Invoke-WebRequest -UseBasicParsing 'https://spotx-official.github.io/run.ps1') -new_theme ""   Invoke-Expression"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	cmd.exe
<b>Information</b> <b>User:</b> admin <b>Company:</b> Microsoft Corporation <b>Integrity Level:</b> MEDIUM <b>Description:</b> Windows PowerShell <b>Exit code:</b> 0 <b>Version:</b> 6.1.7600.16385 (win7_rtm.090713-1255)				

### Registry activity

Total events	Read events	Write events	Delete events
1 232	1 178	54	0

### Modification events

<b>(PID) Process:</b> (2268) powershell.exe	<b>Key:</b> HKEY_CLASSES_ROOT\Local Settings\MuiCache\178\52C64B7E
<b>Operation:</b> write	<b>Name:</b> LanguageList
<b>Value:</b> en-US	

### Files activity

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

### Dropped files

PID	Process	Filename	Type
2268	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\P0YQZ0A0B5UY6PBOXTT2.temp MD5: CAEA3B1F09925DA2A47C2B8B890AB890      SHA256: 66F29B00CBB7B1DED878F96AAC6F52907C088DE194A1FD0CD6E1FF1916047549	binary
2268	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF20185e.TMP MD5: CAEA3B1F09925DA2A47C2B8B890AB890      SHA256: 66F29B00CBB7B1DED878F96AAC6F52907C088DE194A1FD0CD6E1FF1916047549	binary
2268	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms MD5: CAEA3B1F09925DA2A47C2B8B890AB890      SHA256: 66F29B00CBB7B1DED878F96AAC6F52907C088DE194A1FD0CD6E1FF1916047549	binary

### Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	2	0	0

### HTTP requests

No HTTP requests

### Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:138	-	-	-	whitelisted
4	System	192.168.100.255:137	-	-	-	whitelisted

### DNS requests

No data

### Threats

No threats detected

### Debug output strings

---

No debug info



Interactive malware hunting service ANY.RUN  
© 2017-2023 ANY.RUN LLC. ALL RIGHTS RESERVED





