6 Updater

Every several hours or every time a computer is idle, the malware-toolchain updater is executed (i.e. `GUP.exe` and `Convertor.exe`). This is however not an original code of its authors, but it is yet another misusage of a free code[21] that originally served for automatic update of the Notepad++ editor[22].

Based on the PDB debug-info location stored in `GUP.exe`, we can see details about their usage of this tool "`G:\PROJECTS\VolaroTech\UPDATERS_NEW_IDEAS\gup_trunk\bin\GUP.pdb`". We can also see a reference to a string VolaroTech, which is most probably related to Volaro Technologies & Applications[23]. The details will be discussed later.

The task of this updater is quite easy – it reads the location of the latest update from its configuration file (XML), downloads the file, and executes it. Such an XML file is a 1:1 copy of the aforementioned WinGUP project with only one tag modified: `InfoUrl`, e.g.:

```
<?xml version="1.0" ?>
<GUPInput>
  <Version>4.6</Version>
  <InfoUrl>http://usads2.info/hp188s6GT/Z4.php</InfoUrl>
  <ClassName2Close></ClassName2Close>
  <MessageBoxTitle extraCmd="" ecWparam="" ecLparam="">Notepad++ update
</MessageBoxTitle>
  <SilentMode>yes</SilentMode>
</GUPInput>
```

Figure 35 – Updater XML configuration file[24].

Few examples of the other update sites are:

```
http://usttor.info/hV93AwPtrlu/B6.php
http://usdsd1.info/gCd7QYch/jzuFZ.php
http://usads2.info/zPj6FII6u6/jj.php
http://weath4us.info/mC81EyWEc/vb.php
http://weathus1.info/JCWNQ/GX1AA.php
http://weathtoous.info/fhcm5tie8u3w/bzugC.php
```

Such update site (probably running on a GUP server-side[25]) contains information about availability of a new dropper. If the version is newer than the current installation, the file is downloaded and executed.

[21] https://github.com/gup4win/wingup
[22] http://docs.notepad-plus-plus.org/index.php/Auto_Updates
[23] http://www.volarotech.com/
[24] The comments have been removed for a better readability.
[25] http://sourceforge.net/projects/gup/

Serial Number Exeoutput For Php ->->->-> http://shurll.com/75ct8

Terms and Conditions Disclaimer Privacy Policy Copyright 2009 - 2013 serialnumber.inLearn more You're viewing YouTube in EnglishWorks with MySQL and other databasesFolder Lock 7 Version 7.6.1 Serial Key Folder Lock 7 Code 7.1 Serial Ummy Video Downloader 1.7.2.7 Cubase 7 Activation pinga video song download from bajirao mastani movie timesinstmank Serial NumbersSave Sign in to YouTube Sign in No videos in this playlist yet Watch Queue Queue count/total Felix Simmons SubscribeSubscribedUnsubscribe10 Loading

200 serials exeoutput for tone2 nemesis download crack idm 1.7 serial key' Date Name Success Rate 2009-10-23 07:01:25 3ds Max 9 Serial 69% 2009-10-22 23:27:28 AVG 7.0.308 (21.04.05)Serial 24% 2009-10-22 23:27:28 AVG 7.5.516 Serial 11% 2009-10-22 23:44:51 BRD Serial 73% 2009-10-22 23:49:52 Serial Box 0.6.1 70% 2011-09-08 12:46:52 Serial Box 0.6.1 62% 2011-09-08 12:46:52 Serial Box v0.6 1 66% 2012-12-12 02:38:05 ATA serial 40% 2012-12-12 03:59:50 BFH Serial 80% 2012-12-12 13:40:38 GTA IV Serial 69% 2012-12-13 07:14:39 Serial HD 65% 2009-10-17 06:18:30 AggPub 1.0 SERIAL 56% 2009-10-17 06:18:31 Air Messenger Serial V3.7.6 14% 2009-10-17 06:18:52 AquaAngel 3D SERIAL 59% 2009-10-17 06:18:52 AquaButterfly 3D SERIAL 62% 2009-10-17 06:18:52 AquaCoral 3D SERIAL 44% 2009-10-17 06:18:52 AquaFish2.3D SERIAL 51% 2009-10-17 06:18:52 AquaScreen 3D SERIAL 32% 2009-10-17 06:18:52 AquaScreen2.3D SERIAL 58% 2009-10-17 06:18:52 AquaSea 3D SERIAL 51% 2009-10-17 06:18:52 AquaSirene 3D SERIAL 11% 2009-10-17 06:19:08 Avast!.4.6.691 SERIAL 63% 2009-10-17 06:19:28 BD Gest 5.2.2 SERIAL 54% 2009-10-17 06:20:14 CDRipper V2.85 SERIAL 14% 2009-10-17 06:20:25 CleanMantra Ver 1.5 SERIAL 57% 2009-10-17 06:20:25 Cleant It 3.06.11.28 SERIAL 28% 2009-10-17 06:20:38 Compt In V4.0.1 SERIAL 20% 2009-10-17 06:20:39 CopyRator 1.4 SERIAL 23% 2009-10-17 06:21:18 Delenda 2.4.14 SERIAL 72% 2009-10-17 06:21:25 Desktoplet 1.0 SERIAL 47% 2009-10-17 06:21:32 Diondine 5.0 SERIAL 61% 2009-10-17 06:22:21 Espion Pro V6.1.6 SERIAL 66% 2009-10-17 06:22:59 Filerecoveryangel 1.1 SERIAL 37% 2009-10-17 06:22:59 Find It Pro 4.01.11.29 SERIAL 57% 2009-10-17 06:23:00 FishPond SERIAL 20% 2009-10-17 06:23:07 FullDisk V5.3 SERIAL 65% 2009-10-17 06:23:45 GoGoldfish 1.0 SERIAL 21% 2009-10-17 06:23:45 Goleador 5.1 SERIAL 45% 2009-10-17 06:25:01 ICONStudio 5.0 SERIAL 0% 2009-10-17 06:25:01 II Calendar V2.6 SERIAL 0% 2009-10-17 06:25:01 II ColorPicker V2.0 SERIAL 0% 2009-10-17 06:25:01 II QuickMemo V1.5 SERIAL 0% 2009-10-17 06:25:01 II WorkLog4All V4.50 SERIAL 60% 2009-10-17 06:25:01 II WorkProject V4.41 SERIAL 0% 2009-10-17 06:25:01 II WorkProjectPro V2.32 SERIAL 0% 2009-10-17 06:25:01 II WorkSchedule V5.21 SERIAL 54% 2009-10-17 06:25:01 II WorkTimeCloks V1.5 SERIAL 0% 2009-10-17 06:25:11 IncrediZoom 10 SERIAL 30% 2009-10-17 06:25:48 J-Perk 7.0 SERIAL 0% 2009-10-17 06:25:48 paradisebirds anna and nelly avi 5.11 SERIAL 53% 2009-10-17 06:25:48 Jerrycan 6.25 SERIAL 10% 2009-10-17 06:27:05 Loto V1.40 SERIAL 55% 2009-10-17 06:27:05 Loto V1.41 SERIAL 53% 2009-10-17 06:27:05 Loto V1.42 SERIAL 53% 2009-10-17 06:27:46 Magic 3D 2.1 SERIAL 52% 2009-10-17 06:27:46 MagicTweak 2.90 SOME-SERIAL 59% 2009-10-17 06:27:56 video watermark software full versioninstmank 1.0 SERIAL 0% 2009-10-17 06:28:04 MP3 Converter Pro 4.1 SERIAL 0% 2009-10-17 06:28:04 MP3Coder V1.65 SERIAL 0% 2009-10-17 06:28:08 MURENES SERIAL 33% 2009-10-17 06:29:19 One-to-One Meetings V1.0.10 SERIAL 0% 2009-10-17 06:29:58 Palette V3.2 SERIAL 0% 2009-10-17 06:29:58 Part It V3.01.12.01 SERIAL 0% 2009-10-17 06:29:59 PC Watcher 1.0 SERIAL 58% 2009-10-17 06:30:06 PhotoToFilm V2.5.0.56 SERIAL 20% 2009-10-17 06:30:07 Picturecollagesoftware SERIAL 51% 2009-10-17 06:30:11 PolyView 4.28 SERIAL 0% 2009-10-17 06:30:18 Print It 1.04.02.08 SERIAL 0% 2009-10-17 06:30:19 PuzzleFX 2.0.(3.0) SERIAL 73% 2009-10-17 06:31:33 REQUINS SERIAL 9% 2009-10-17 06:31:33 RippedRadio 2.01 SERIAL 0% 2009-10-17 06:32:11 ScanToEmail 3.13 SERIAL 0% 2009-10-17 06:32:11 ScanToPDF 3.13 SERIAL 35% 2009-10-17 06:32:15 SDAquarium 3D SERIAL 0% 2009-10-17 06:32:15 ShowMe 1.8 SERIAL 53% 2009-10-17 06:32:15 Shred It 1.01.11.28 SERIAL 0% 2009-10-17 06:32:40 Spy Stalker 1.0.1 SERIAL 0% 2009-10-17 06:32:40 Stamp It 5.01.11.28 SERIAL 0% 2009-10-17 06:33:27 TORTUES SERIAL 13% 2009-10-17 06:35:38 Watcher 2.30 SERIAL 25% 2009-10-17 06:35:38 WATTERFALL 3D SERIAL 0% 2009-10-17 06:35:38 WatterFallGreat ediabas inpa download deutsch SERIAL 0% 2009-10-17 06:35:38 Web Confidential 3.1.0.0 SERIAL 60% 2009-10-17 06:35:44 Willing Webcam 2.8 SERIAL 67% 2009-10-17 06:35:44 Willing Webcam 3.0

SERIAL 35% 2009-10-17 06:35:48 Wipe It 1.01.11.28 SERIAL 0% 2009-10-17 06:35:49 WordFree PDF V1.1.0.2 SERIAL 0% 2009-10-22 23:27:13 Ad-Aware PRO 7 Serial 50% 2009-10-22 23:27:15 Age Of Mythology Serial [Sum Up] 43% 2009-10-22 23:27:16 Air Messenger Serial V3.7.6 0% 2009-10-22 23:27:16 Air Messenger Serial V4.0 0% 2009-10-22 23:27:27 Avast Pro Serial 76% 2009-10-22 23:27:27 AVG 6.0 Original Serial 40% 2009-10-22 23:44:49 BitDefenderInternetSecurityv.10+Serial kashmir ki kali full movie download 2009-10-22 23:45:49 Carrara 4 Pro Serial 0% 2009-10-22 23:45:52 CloneCD 4.9 (SERIAL) 0% 2009-10-22 23:46:26 DFX 8.5 Working Serial 62% 2009-10-22 23:46:27 Die Sims 2 Serial 0% 2009-10-22 23:46:29 DSJ 3 1.4.0 Serial Work!! 0% 2009-10-22 23:47:51 Finalcut Pro 5.1 Serial 56% 2009-10-22 23:47:53 FREE SERIAL AVG 8.138 86% 2009-10-22 23:47:59 Gangland Serial 0% 2009-10-22 23:48:07 HelpBlocks 1.21 Serial 0% 2009-10-22 23:48:18 IsoBuster 2.5 Serial 40% 2009-10-22 23:48:18 IuVCR Serial (verTags: flash, application, extensions, compiler, runtime, software, html, windows, visual, exeoutput.com - daily visitors: 1,476 pagerank: 3/10 The most RAD framework for PHP li3 li3 is the first and only major PHP framework built from the ground up for PHP 5.3+, and the first to break ground into major new technologiesExternal Search Try finding Exeoutput For Php steinberg hypersonic 2 crack torrent download at our partner sites: WarezCore and IceDDL.Template for Jenkins Jobs for PHP Projects The goal of this project is to provide a standard template for Jenkins jobs for PHP projectsLanguage: English Content location: Ukraine Restricted Mode: Off History Help LoadingSoftware - Home Site G.D.GExeOutput for PHP 1.7.0 Portable r3021 is compatible with all windows 64 bit and 32 bit.TagsDownload ExeOutput for PHP 1.7.0 Portable r3021ExeOutput for PHP 1.7.0 Portable r3021 DownloadExeOutput for PHP 1.7.0 Portable r3021 CrackedExeOutput for PHP 1.7.0 Portable r3021 PatchExeOutput for PHP 1.7.0 Portable r3021 NulledExeOutput for PHP 1.7.0 Portable r3021 TorrentExeOutput for PHP 1.7.0 Portable r3021 No SurveyExeOutput for PHP 1.7.0 Portable r3021 Full versionHow to ExeOutput for PHP 1.7.0 Portable r3021 InstallHow to download ExeOutput for PHP 1.7.0 Portable r3021ExeOutput motivational books in hindi free download pdf PHP 1.7.0 Portable r3021 warhammer mark of chaos no-cd crack FreeExeOutput for PHP 1.7.0 Portable r3021 Relient K-Mmhmm full album zip keyExeOutput for PHP 1.7.0 Portable r3021 key generatorkeygen for ExeOutput for PHP 1.7.0 Portable r3021serial for ExeOutput for PHP 1.7.0 Portable r3021ExeOutput for PHP 1.7.0 Portable r3021 username passwordactivation ExeOutput for PHP 1.7.0 Portable r3021full activator ExeOutput for PHP 1.7.0 Portable r3021ExeOutput for PHP 1.7.0 Portable r3021 launcherExeOutput for PHP 1.7.0 Portable r3021 for WindowsExeOutput for PHP 1.7.0 Portable r3021 MediafireExeOutput for PHP 1.7.0 Portable r3021 ThePirateBayExeOutput for PHP 1.7.0 Portable r3021 cnetExeOutput for PHP 1.7.0 Portable r3021 RapidshareExeOutput for PHP 1.7.0 Portable r3021 Direct downloadExeOutput for PHP 1.7.0 Portable r3021 update0day ExeOutput for PHP 1.7.0 Portable r3021ExeOutput for PHP 1.7.0 Portable r3021 License codeExeOutput for PHP 1.7.0 Portable r3021 GeneratorExeOutput for PHP 1.7.0 Portable r3021 CrackGet ExeOutput for PHP 1.7.0 Portable r3021 PatchExeOutput for PHP 1.7.0 Portable r3021 GratisGratuit ExeOutput for PHP 1.7.0 Portable r3021Tlcharger ExeOutput for PHP 1.7.0 Portable r3021 less Click the Link to Download - Legit ExeOutput for PHP 1.7.0 Portable r3021 Download Free with Keygen License Key Crack Patch SerialClick the Link to Downloa

scripts and PHP websitesLoadingGlad you sign in able to the Windows Index Experience Base CreditPc Performer 11.10.1.2646 Serial Key Ser Cubase 7 Activation Code Serial NumbersThese infections might corrupt your computer installation or breach your privacyexeoutput Software - Free Download exeoutput - Top 4 Download Link to us Tell-a-friend Contact Software Scripts Drivers RSS BOOKMARK Toggle navigation Featured Software New Software Top Downloads Must-Have Downloads Coupons Reviews Submit Software PHP HTML Editor,online HTML Editor,PHP WYSIWYG,WYSIWYG HTML Editor,PHP Text Editor,PHP Editor CuteEditor for PHP - a powerful PHP HTML Editor, .NET and ASP version is available Tags: php, editor, online wysiwyg html editor, cute editor for php, php html online html editor, content, php wysiwyg editor online, noteeditor php, wysiwyg html editor web based download, phphtmledit.com - daily visitors: 1,333 pagerank: 3/10 trustworthy: 64/100 Themes for PHP-Nuke and WordPress Free and Commercial Templates for PHP-Nuke portals and WordPress blogs Tags: php nuke themes, phpnuke theme, nuke griffin, neko wordpress theme, nuke template free download, free phpnuke theme, php dolphin themes, php free theme, nuke themes free, php nuke themes free download, kalgash.com - daily visitors: 19

pagerank: 4/10 Click "Save" next to each software to save it hereHTML Executable is a versatile electronic publication and ebook authoring solution with powerful features

Aug 28, 2013 File Size: 2.25 Web Tamarin - A blog for PHP/MySql developers A blog for PHP/MySql developers Tags: google directions, mk slider, wordpress mk, webtamarin.com - daily visitors: 100 PHP-DI - The Dependency Injection Container for humans PHP-DI is a Dependency Injection Container for PHP that intends to be practical and powerful Tags: php di, php container, php dependency injection, dependency injection php, php-di.org - daily visitors: 333 Tags: itunes, seo website, amazon, video, hover arcades script, games amazon portal script, portal store script, facebook social exchange, kool-heads.com - daily visitors: 1,143 pagerank: 1/10 e1977f8242