ID: 752911
Sample Name:
PWMinderInstaller-3.3.1.1.msi
Cookbook: default.jbs
Time: 00:43:00
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

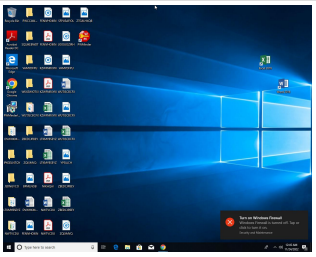
Windows Analysis Report

PWMinderInstaller-3.3.1.1.msi

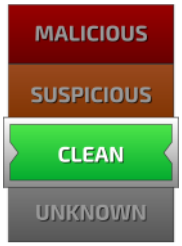
Overview

General Information

Sample Name:	PWMinderInstaller-3.3.1.1.msi
Analysis ID:	752911
MD5:	9661ec2a8a20c9..
SHA1:	092ee11b9c2805..
SHA256:	d621d35135fe84..
Infos:	



Detection

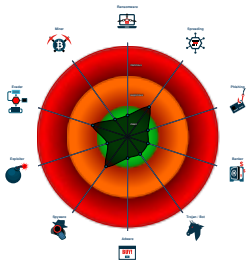


Score:	13
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Creates autostart registry keys to la…
- Drops files with a non-matching file …
- PE file does not import any functions
- Queries the volume information (nam…
- Adds / modifies Windows certificates
- Drops PE files
- Tries to load missing DLLs
- Deletes files inside the Windows fol…
- Drops PE files to the windows direc…
- Creates files inside the system direc…
- Binary contains a suspicious time s…
- Stores files to the Windows start me…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Process Tree

- **System is w10x64**
- msiexec.exe (PID: 6044 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\PWMinderInstaller-3.3.1.1.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 6096 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 1348 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 483844CA7CD225D329998D5B1C5B7780 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - msiexec.exe (PID: 6048 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding BD76792E804F7BE88D040374A60ADC55 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

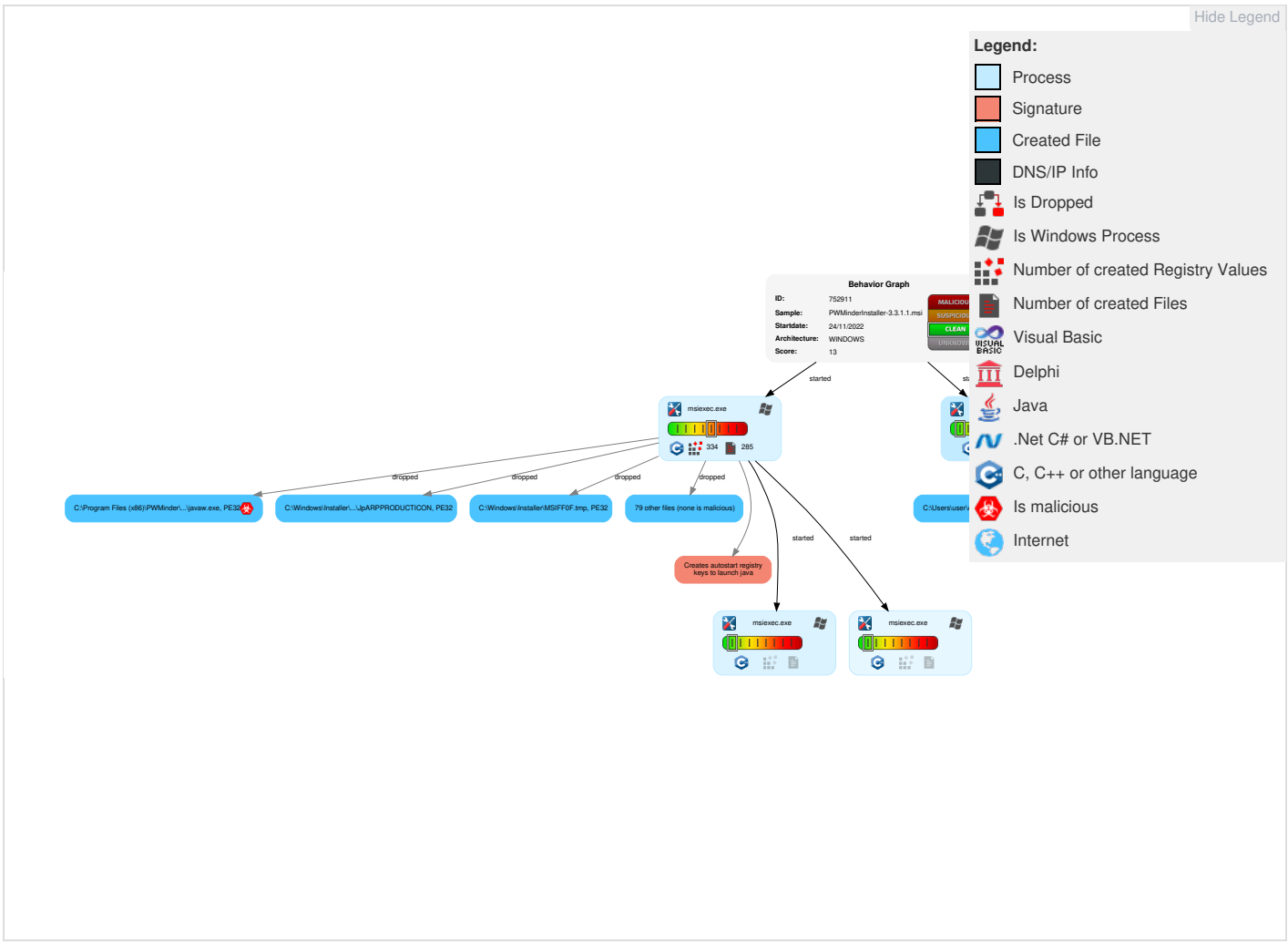
Boot Survival

Creates autostart registry keys to launch java

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	Windows Management Instrumentation	1 Windows Service	1 Windows Service	3 2 Masquerading	OS Credential Dumping	1 Process Discovery	1 Replication Through Removable Media	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 1 Registry Run Keys / Startup Folder	1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 DLL Side-Loading	1 1 Registry Run Keys / Startup Folder	1 Process Injection	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 Timestomp	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

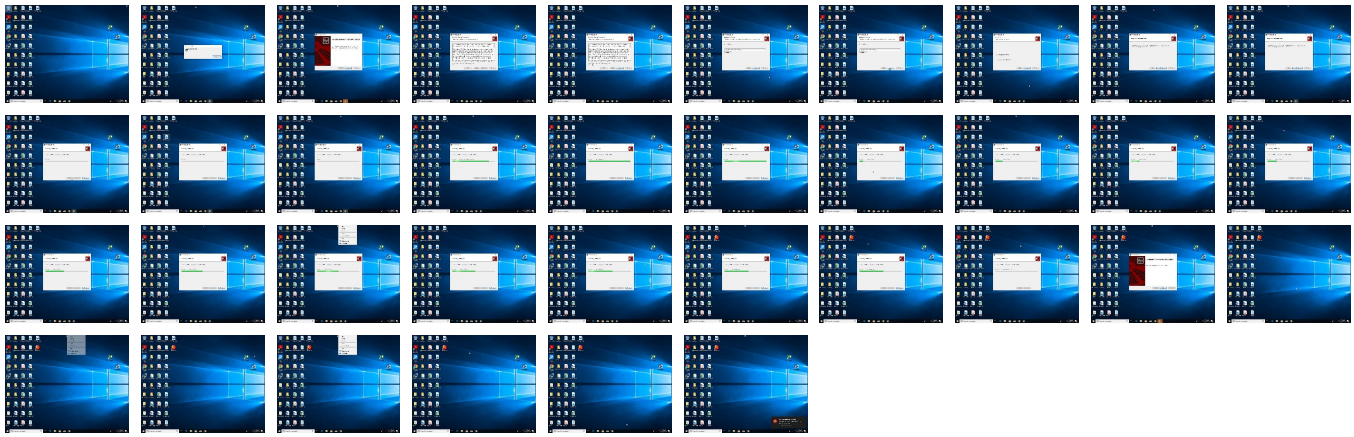
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\PWMinder\runtime\bin\API-MS-Win-core-xstate-l2-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-console-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-console-l1-2-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-datetime-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-debug-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-errorhandling-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-fibers-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-file-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-libraryloader-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-localization-l1-2-0.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-memory-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-namedpipe-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-processenvironment-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-processthreads-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-processthreads-l1-1-1.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-profile-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-rtlsupport-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-string-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-synch-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-synch-l1-2-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-sysinfo-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-timezone-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-util-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-conio-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-convert-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-environment-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-filesystem-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-locale-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-math-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-multibyte-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-private-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-process-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-runtime-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-stdio-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-string-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-time-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-utility-l1-1-0.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\awt.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\client\jvm.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\dna.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\fontmanager.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\freetype.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\j2gss.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\java.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\java.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\javajpeg.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\javaw.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\jawt.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\jimage.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\jli.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\jrunscript.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\jsound.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\keytool.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\kinit.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\klist.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\ktab.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\lcms.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\management.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\mlib_image.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\msvcp140.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\net.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\nio.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\prefs.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\rmi.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\rmiregistry.exe	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\server\jvm.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\splashscreen.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\sspi_bridge.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\PWMinder\runtime\bin\ucrtbase.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\vcruntime140.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\verify.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\w2k_lsa_auth.dll	0%	ReversingLabs		
C:\Program Files (x86)\PWMinder\runtime\bin\zip.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIBC68.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIC0BF.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIFF0F.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	752911
Start date and time:	2022-11-24 00:43:00 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PWMinderInstaller-3.3.1.1.msi
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean13.winMSI@6/240@0/0

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: PWMinderInstaller-3.3.1.1.msi

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\63e8f8.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	57586
Entropy (8bit):	5.901024503613299
Encrypted:	false
SSDEEP:	768:MLe6BxCsT0d66FfrZVqiJPl5nhEGjnmwXn:tikK0d66FfrZ5p6GVXn
MD5:	ED6EBDB3C6E3EA2AA0C86E8D460F8B09
SHA1:	9B5FC0A522DA5F75E0CBE1E3C73CBCD02EF9963C

SHA-256:	452DB483B257F63390FF7D31C0E48EFA2F727515F5289EBAB3709B5F88372AFE
SHA-512:	615698E5A9313EEFFE52C58A4704056EF8A75783F69F8D2E96CBCB6E03FACFEE07F60A589654C3D40C4F1EB15BEC2792953F81712C4ED22C61D966EBA5745146
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@..xU.@.....@.....@.....@.....@.....@.....&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}..PWMinder..PWMinderInstaller-3.3.1.1.msi.@.....@.....@.....@.....JpARPPRODUCTICON..&.{5EB4ACF9-60F1-4E53-B837-23C8A24DDA3A}.....@.....@.....@.....@.....@.....@.....@.....@.....@.....PWMinder.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{F2C5738A-0188-329A-96D3-4D099A819786}&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}.@.....&.{22B8464C-9858-34F2-B091-289D8ED6C2DA}&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}.@.....&.{DF844933-25D0-331C-9ECF-75E7149EBA38}&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}.@.....&.{E3E0FA64-2A7F-318D-B4E6-75275DA8A5C3}&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}.@.....&.{E59A3803-A0DD-34B5-A320-916FEF733F8A}&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}.@.....&.{7EE9AD88-BF40-3365-8B6C-CED645142A01}&.{057BD86F-54F3-343C-AD7C-A5491C1BF591}.@.....&.{3E9B44E6-8194-3344-B82B-209EE8AD

C:\Program Files (x86)\PWMinder\PWMinder.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	534896
Entropy (8bit):	6.272752879884908
Encrypted:	false
SSDEEP:	6144:bLxjgQWziAfsZqCNzuGzFU8SmfAOCA2Hk8GGGwhECKu2xq2wxmm:npWziAfsZDq+UfEs2xq2wxB
MD5:	70A3C9C307218D28ADA05803643C2B10
SHA1:	A105753F73D5068DC6416E533AB2E51BF23A2060
SHA-256:	1499B9DCD5B223A2BFEE521FC9FDC4C440E60286C54AC631D3DA9575CD787932
SHA-512:	038184A2650C1935374D6C67F742CC625E77AFA8ED19A83EAAA114C2CA5AC248B4A6ECF5FD757D770775E9F52283FFBA5C0D1D5CD2E9A2E9C8F49E4B19934ADD
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'@.t@.t@.t...uO.t...u..t...uV.t...uM.t@.t..t...uQ.t...uT.t...u..t...uA.t...uS.t...uA.t..gtA.t...uA.tRich@.t.....PE..L.....?.....j.....L.....@.....0.....I....@.....`.....P.....`.....p).....-...T..p.....`U..@.....text....h.....j..... ..`.rdata...+.....,...n.....@..@.data....&.....@....rsrc...`..... .....@..@.reloc...-.....@..B.....

C:\Program Files (x86)\PWMinder\PWMinder.ico

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 10 icons, 256x256 with PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced, 32 bits/pixel, -128x-128, 32 bits/pixel
Category:	dropped
Size (bytes):	200735
Entropy (8bit):	5.216368656784317
Encrypted:	false
SSDEEP:	1536:+Rmdp8eEtQgEwpLGGG4EU4RMr6XzKE6kERRTEZIASLNT0+9NKZfj:+R8eBqAGGGDULIE6PRRwZuYZb
MD5:	2F6FC0D077719768CBF4E665E87B2AAD
SHA1:	C0147734DEFD436D780DCB0CEA0B72B291D671A8
SHA-256:	4C6F8D73849A354FDB1D89FD93BDF83C7EE5DA2605CCE4AF3849DE1C9C8D5E3C
SHA-512:	20D3E2F532C2F88401B2A05CF624F49561F51CA1E7612906C592D06E3D67A22C021C020DFF37D37FD0DCD85A369CA73C66FF3994BD24483A997779C24F712CD
Malicious:	false
Reputation:	low
Preview:	..... .lp..... .(....p..00.... ..%...y.. .... .h...g.....pg.....(...?...00.....g... .....h.....PNG.....IHDR.....\r.f....sRGB.....gAMA.....a....pHYs.....o.d..o.IDATx..].xTU.~g&..B.$$$.....b....e.(`A. 6l.. *.....6zG....i.g....wKr....;....<.a.{..9.{.....n..n..fp...m.]......|...^..6P....8Ok}....].....5j.F:U.{.....m....O.>o.m..w.m.....3g.4e.E..&..._~.e.u.].]UU...n.....N....m.e.\s.5.....sgS{.}'...t[.t..k....n...../<A.E..p...b.qW_}..*++}.w....^zi...3...4....%.....}L&|4z4...`.8..a.G.....S7.<g...o..:.....V.....R..z.....i.^u.I7.8l.V..s.W...~..|2n..EG..F....h.=uuM....-G".L.....M.:u..N...f.P....+**.....bxL....5.Y.#.^...3.I..N.x..._.....r..Ym.5.....M...+.....g}'g...V..vV.H .....2y...;.&..z..$..V.?..W_.Q.:...6...G..J.n.....]R.jm.E.M.4i....M..UW].Syy....?..z...Y;.%....>.ywSm.....x....H.m7....u.F\~..?...d..7.Q]...v=..A..CS.gy-$"..H..!. ..V..H

C:\Program Files (x86)\PWMinder\app\EaSynthLookAndFeel.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	89746
Entropy (8bit):	7.590465385089637
Encrypted:	false
SSDEEP:	1536:PDUbtaVrhHHnnCi/QPKknV07SmGd9X1dIksVNZXOnGwthjKKJK:bUkVrtiigKknW7SmUdI1ZXWjhuP
MD5:	AB9DACE5C381013951A6036E74BBD28D
SHA1:	39A722F6FF96E8C9C0A11629B16E51BAFCDC4B75

SHA-256:	F91E89A2B4FD70F081442D13F1E0E6541801EDCF6CCF3AFC7F0993175B0765B1
SHA-512:	70756ACF23F21D68850C46D0C7762C41B4CD99BF9D4A43467800676DF51CA9D3984BD1D7A15A97B872EED4B00FD506DD4281CDB2FB583E4867A3354B6B08A9 6
Malicious:	false
Reputation:	low
Preview:	PK.....<.....META-INF/MANIFEST.MF....M....0.D.....7.-....B.AW...1...7..zZv..3{.${4.5...).....!.I..ji..p..Fv.\...upET.D<..`...v)U..Z..(.p.\G.....E..e.pqYI.*..Te.....H 9...R. ../_.H.YF...o.....vDHf...x.N..a..PK..vYpM.....PK.....<.....#...com/easynth/lookandfeel/easynth.xml.][s.8.~...\...V..;....K...Ko.t....h....T.._..$A.7R...8=5.....e.- .V.....g.z...M...fwFY}['.}.^...sb.."1.U\.q..X.m.%YU.....Y-VFl..d.....U.%AE..6.+R23~..F'...sR|.~...m.UF.o..{.....L....O^....?.E.[..*..X&Et..."...u.<1..,_..3.....j... ?.L...+._.....\ .....?..^.8:...2..%)4.....s.m>.e*...,u&m8.?...`.....&eZ}v.m.8..;.p....p.M.....j3....+.....3.=....I./.*).x..@.1z....\C0.I.s8q...B.Cg.:.Z...g...j<!(jb..|...7.s.oV.?(.....tY$.'.x.K.....E|....".E..J.eC 22..$.&v.L...C#.....m..M/..;Z._..[Rq.k.....4[...`:1Er...../`...P....F\...q....Z.....1.....rR<.+.,..}....\...B...p.6I...q....S....2-., .^.dyQ....}RV...w.....ZVq...|.....

C:\Program Files (x86)\PWMinder\app\LGoodDatePicker-11.2.1.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	338734
Entropy (8bit):	7.881643301890838
Encrypted:	false
SSDEEP:	6144:aH5b6djt/DyW1Z1+SznqfVsqKhGu3MpBW6DWlWvXhgAfw:al+8WnB29PK0u3Mp86DWCeAY
MD5:	DA308F9FB736857875F1A8986813A089
SHA1:	D4FE83557D1E38CB0F1EC29B867C3A59FC0DFC1D
SHA-256:	2FA8252F3292286376A32B5494F72890EC6A2DF85E36D295960098D8DD5F8092
SHA-512:	5D7C80DF1039DF1714D16F0F4F727C8CAEFE5AFF21D1B7462C049D7EB2A16E72340FFECDFF889878DB2DD3122EF821BC63C63EE0ADC2822630D380F8271C70 7
Malicious:	false
Preview:	PK.....aR.....META-INF/.....PK.....PK.....aR.....META-INF/MANIFEST.MF...j.0.E....~@".*x.;....E.L.I<D...I..J.d.B.n..9s..O.LY.aL.|#...u..A&-.`.E.....#.| ({....8.>a.H.#.....$..p...Y...x}...../.E.....E.3....9]....}.Zr..y.YH.V+e...\...3...C.h..}N..O..%.0.I..s.X....c...v`....x.7._PK..../-...;...PK.....aR.....com/..PK.....PK..... ..aR.....com/privatejgoodies/..PK.....PK.....aR.....com/privatejgoodies/forms/..PK.....PK.....aR.....!...com/privatejgoodies/forms/la yout/..PK.....PK.....aR.....2...com/privatejgoodies/forms/layout/BoundedSize.class.Vmo.U.~n.e..,K[[.8"..K. /.....T..Rh.M..N.Sfg.y).?.G....~3..~...H.....D.F..? @D.....;.s.s.....(.q4.cQ...z.p..'.0*a,.....*.q:.38.sQ.~...p....!..y...hQ4.Qy....$...t.S.....I.*fJ.>....e.....1...fF.+Z.C..iv.....J..p.n..>.....%F....:...W.i..5g.%...1..:....n.'...

C:\Program Files (x86)\PWMinder\app\PWMinder-3.3.1.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	4140772
Entropy (8bit):	7.988310747239917
Encrypted:	false
SSDEEP:	98304:jyMa8uMQFGaGoujGNk1td7oujGNk1tQOSp2vmgb3bQ3qznkYE8w8:jWIBaUqkbdNqkbQHpFG3Uq7kD83
MD5:	3A948CAAAFB31D4F8785CB32D8A159CA
SHA1:	472D09688B73A5D980DE71CF14726BB5EBD59B81
SHA-256:	C37DA7828BD3A368284E43C151EF862726FBA446E55CAED1BB37876617B93A4C
SHA-512:	93EDA9C575E678960C81F346A3774A5114CB6AB4A2C3AAADCC3490FA5CBF80461EE21BE7ED0A5BC1D36F2F4E25453815644D163F9D050094188B74C5B7D4B7 8
Malicious:	false
Preview:	PK.....|zqUs.....META-INF/MANIFEST.MF-...0.@.=_.F..H(.....8Tt...c.lJ._o...p...b*n...N.@...T4...H!.....?.....K.(...J..>..-A....+N.5?k.X.b..,.SL.+8....vi%..~. ....>.5c? PK.....|zqU[-..G.....ca/ewert/pwMinder/a.class}W[s.E..f...6..l.@.+7...r.....Bd..d3$.fg..YH....w.V...(.JJ..A-_.....&N..t...;.9}.{..??..`/>..}..k.....5...j05x.^....w4...=..h. H.'*r*...V1..K*..xQ.K*^V....a.h.E.l..V....E.H...-.=Qt.)]...2a]..Qt.)=..]...b%..p..E...Y<...C.9..8.c.....l<...'b(.`....8...8. ...XW.}..5.K.."J..wC:.....FL{.pS...eJ?..L'5l.J^.s.=O..... iG..:.....'8.\.../u..0..z7.*...t"L.{.....z.ewiNj..D/.....2r^.cm g...=..~.....c.S`>M../V)..9..l..z...V...!.d.'l.Kp.. ..Y..(T.R.<.. zp:g.<.`.k..[.6m.H)?f.'.1..3..3..Z...u..J.i.....NN.Fu..n\|_.Srs.!S(..O.....QaF4..o.y..z.t\....)h..HA,g9E.x.4<kF..s....s.3.91.....G.&c.3\[...J.....`YW..;..=*.<.....7S.N.E..+.Zf.....I~...i.i/.X..x.bx.m8Z.H.N....YX.....+j.....5.j'..$.6v.>.[.....Y..T.

C:\Program Files (x86)\PWMinder\app\PWMinder.cfg

Process:	C:\Windows\System32\msiexec.exe
File Type:	Generic INItialization configuration [JavaOptions]
Category:	dropped
Size (bytes):	1718
Entropy (8bit):	4.993727548091234
Encrypted:	false
SSDEEP:	24:1vgTSRngBjI0mm7VeNPevIqj5OgYS47iY:NgTSRngllz6egixGh
MD5:	35129E80446AE0A27B0D017C04B730F9
SHA1:	F50F14155297058CB02A540C6078C7EA14A8FE79
SHA-256:	9400A089252C669EF2F12075D7B557C445DD3C8EFE42F61D7CAB0F151A583E00
SHA-512:	6CE668FD148F5CEDFCA060EE44EE564DE3AC314AD12E7C898E8F161086333BA388CAA64489BD571DB1ACF0AB7BD2743EE1A36E7EDA114FDDD5AA00E9C04E 0A20

Malicious:	false
Preview:	[Application]..app.classpath=$APPDIR\PWMinder-3.3.1.jar..app.mainclass=ca.ewert.pwMinder.MainProgram..app.classpath=$APPDIR\bcprov-ext-jdk15on-1.60.jar..app.classpath=$APPDIR\bcprov-jdk15on-1.60.jar..app.classpath=$APPDIR\commons-codec-1.15.jar..app.classpath=$APPDIR\commons-httpclient-3.1.jar..app.classpath=$APPDIR\commons-io-2.11.0.jar..app.classpath=$APPDIR\commons-lang3-3.12.0.jar..app.classpath=$APPDIR\commons-logging-1.2.jar..app.classpath=$APPDIR\custom-components-2.0.0.jar..app.classpath=$APPDIR\dropbox-core-sdk-5.4.4.jar..app.classpath=$APPDIR\EaSynthLookAndFeel.jar..app.classpath=$APPDIR\flatlaf-2.6.jar..app.classpath=$APPDIR\flatlaf-jide-oss-2.6.jar..app.classpath=$APPDIR\gson-2.9.1.jar..app.classpath=$APPDIR\httpclient-4.5.13.jar..app.classpath=$APPDIR\httpcore-4.4.15.jar..app.classpath=$APPDIR\jackson-core-2.7.9.jar..app.classpath=$APPDIR\jasypt-1.9.3.jar..app.classpath=$APPDIR\javax.activation-1.2.0.jar..app.classpath=$APPDIR\jaxen-1.1.6.jar..app.classpath=$APPDIR\jdom2-2

C:\Program Files (x86)\PWMinder\app\bcprov-ext-jdk15on-1.60.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	4260066
Entropy (8bit):	7.857130979987582
Encrypted:	false
SSDEEP:	98304:m7blb+pRKyrEW1W3FbnZKhvpsVXT5aobW14bYmI:YbryIW1qK0FfLI
MD5:	C80A49D3E1075C44923570EAC95DE3D7
SHA1:	0FAEA4C950BBFA6E8882830F0266BC9185755D37
SHA-256:	2D927919BF4AD006174D4E9B490B795C557F8A66F62F07A18E7C4D50A48D3E51
SHA-512:	CEB045DA4EAC4FCCE1B081131BDC281404C5D2AF5B284C4E1EEDFA5F4494BA7E391B9E01554B17AA90ADBA282F5B32ADAA52DF749889DB4DA0E2AB8101272D60
Malicious:	false
Preview:	PK.....L.....META-INF/MANIFEST.MF.....Y....z?#.?T..}...Nl.uA' ..(....G:..~..G?..c..q"**3...m..E0b.....~...o.7...K.d.?.a.....l..>$el.....__..1._.....<.....s;.....{F.m..8y....cu?.=T;...o.....8...N.f.....f.j.y`...[..y.....hx..8..c;P...,r.w;N.....v.....;..>..w;....Ol.z..8?[.o.|...=.p..n....U...w..8.ZB..MG..6.^.....N.$..[k...%.~.:....(.[.U...)>.;.....l..W....~...).LH.8?....?n.[.Oe....o.aZh....xX.u..T;}...9.q~....._n\~GD.W.....P_...o..yzh..8.#.?...r..z~...]..:d;...`..>~...{..z.O....._.....T.["..<q.d..'..p....r.w....px...!.....9..}...q.=...qx.P_9.....0.M.....2F;N....5._..-;..[F.-..8..~.~{...r..B.#?.l.v.t..}..u.n=.o.;.....4.0..<..b..o..O.....P..Oo ..p...DF.VU..Z....n.O.P....._CC.....6.....#B..g.....[..Si.....}....w.7uQ;...'~...|..O.OL..\g.1R..7..#;.*.....a..).q.g.....4.:..y.....>Z.].....q.<{....?.....L../.y_P@w...?..W=X<.-.i.....=.....}.....o.1.o.*....

C:\Program Files (x86)\PWMinder\app\bcprov-jdk15on-1.60.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	4189874
Entropy (8bit):	7.856493048903261
Encrypted:	false
SSDEEP:	98304:/TWRD2llQfWwFd6tyhvpgB2a5a+1WhQZNmW:/m2rQfayIEgGW
MD5:	435FF931AF9ED4430D2A27456B0386B2
SHA1:	BD47AD3BD14B8E82595C7ADAA143501E60842A84
SHA-256:	7F1A0E6BADAB38666F8467A9A0EE96656B2F8EC8623867ED34F3CDC173B7EE07
SHA-512:	1C08D82349E333720C08FC467FF6489B14B8633A09019BF8BB5E6A3C426DFAE6DCC415648FE1FB4A2DA8631548F4947AB6CA1BC90B3190A05040F4D2EB271A1
Malicious:	false
Preview:	PK.....L.....META-INF/MANIFEST.MF.....W....7z...;t.....$1.]....A...f...$I...p.9...>.....w..{kg...../..&Y.d.G...g....I...i.Eh.O.....k.....???.?en.....xY.a.(.....'...yp..G..j..u...s0....._...{..`...W.8...pw..8...7...o...sl....E.....8...n..=c...o.....a..S...S...A;...6?.`G.?\..l.y|.....D;.SKH{.....y]...].i..Yrsk.8O_...W.z...J....X.....}G|=...<)...C:..O..#._....'.....mv.....5L..8.....n_.j.o.7.4G;....y.....gD...../~..q...6.....G.....x..J..!.q.1.vk.....9....AI|..;..}-O..u.N.~....ORQ/n.|3K..y.U;.0x..?.6?.....>./.h<.....Q...<...a....{...?..wN|....c.?..~.1.q.4.S.....o.)/..2..(j.|r.a...~n.~.1.....M.....,.z...vh.Y..4.4.7<..b..o..O.....P..Oo .p...DF.VU..Z....n.O.P....._CC.....6..~.%./.G.../q.v..o;N..._...}...*....8...wo.v..x._.....8N?!.0....c..~o..mGv.]H../?...S.....+H..-i.}....2....u.n.8.....y.<{.....L../.y.P@w...?..W=X<.-i.....=.....9L.....c._.U.&...O.

C:\Program Files (x86)\PWMinder\app\commons-codec-1.15.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	353793
Entropy (8bit):	7.908532600005254
Encrypted:	false
SSDEEP:	6144:clDdXraL6MLAdTAR5JV4WtBTvEYc6xymTWZaJlQ1V0n34Pw2z:MrqxLA9AR5JV4Wte1mTQ2tld
MD5:	303BAF002CE6D382198090AEDD9D79A2
SHA1:	49D94806B6E3DC933DACBD8ACB0FDBAB8EBD1E5D
SHA-256:	B3E9F6D63A790109BF0D056611FBED1CF69055826DEFEB9894A71369D246ED63
SHA-512:	DA30A7167707 95FCE390E4DD340A8B728F220C6572383FFEF55BD5839655D5611FCC06128B2144F6CDCB36F53072A12EC80B04AFEE787665E7AD0B6E888A678
Malicious:	false

Preview:	PK.....Hy6PZ.....oM.....META-INF/MANIFEST.MF.\Ko.F..... |X.fF..v...[.`.XN`){5Zdk.k.9.%...I...)]...?V....aY...j.o^.I.]...Ypr}8.....U...]R..".xd.....g....(8.Tgq.W..eT$.J...tW...I.. (....L.V!.N.,...!..P\....C^....I^...V.eu..Y.~b%...\./..b....K.ax..,...(....K..$..sX.<.y..I..iX..=.....2....t&..<My$o.?..}..*...$.....T...up.r..$Z..q-.....k.b.f.a.a.:...s...W..X^l6.....x.6./7../...^...g.... n.....r?.{..w...~I..'.G.%.I..3..b$....zd.....e..,^}fe%....X.....w.w..O.....:.42....y.X.Q.k."?.b3.....n.:.:....."j.in.ao..e.Z..&>.B.%..CYD.....d...(7$...j.cZp..r.M.JT}+....^.`\|{.....4... ]....0r....8n..!{..e;6.B3....T3.I..%%3dC..q./..[.g..@.(j.h..`_.R.=....G....)S...&..#W..N...c.$..>...L.1]!pfZ.....P1..>..v.t...o..@+i.H0..f....d.;.?&EZ.e.....Q.q.H.$p.wr[..O.....~R.T^.3..z .^..L....w.-2.....z.,eG..`...K."O`q.....1/.zW..N..C.'.c.....nl..g.?*.=.]F6.....0..k"&.;.{..:....cyi.Q\.y.Z.....B..Vu.....?Sg...._.5.Z..4.....6...,....A...L*.&R..SS..zL

C:\Program Files (x86)\PWMinder\app\commons-httpclient-3.1.jar	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	305001
Entropy (8bit):	7.928644627609034
Encrypted:	false
SSDEEP:	6144:p+XL+YxIBmM8zRgi4S5XKzNFp4z7tTSB1NmV:pyisiKv7tE1MV
MD5:	8AD8C9229EF2D59AB9F59F7050E846A5
SHA1:	964CD74171F427720480EFDEC40A7C7F6E58426A
SHA-256:	DBD4953D013E10E7C1CC3701A3E6CCD8C950C892F08D804FABFAC21705930443
SHA-512:	85E79D4FDB266861910EF95BCD6E82A7F091C9BFBC63DBE2112383EA4D53A5B7A378B54E7C472FBDFDE923F30C72D9CAD626F8FABB0B9C70D1DFB095ADD73 359
Malicious:	false
Preview:	PK.....X.7.....META-INF/....PK.....X.7@./.....D.....META-INF/MANIFEST.MF...N.0..wK~..0.M.....).K...2.%.p...}{...@.....s&...E...jg.X,"J.v.l....o.x)..$.$B.W._ .h...)....,...".-K...:mp.....L.....)..A..._..0s.\];.....2.,Rr.`{...\..8.b...(]j%.W6.Mp..Yz.,..v...Ga..p....+.Uz`.....Ri...C./....M.O....c?... .<.p.F.....bZ.H_.NJ...PK.....eW.7..... ....org/PK.....eW.7.....org/apache/PK.....eW.7.....org/apache/commons/PK.....eW.7.....org/apache/commons/httpclient/PK.....eW.7.....#...or g/apache/commons/httpclient/auth/PK.....eW.7.....%...org/apache/commons/httpclient/cookie/PK.....eW.7.....&...org/apache/commons/httpclient/methods/PK .....eW.7.....0...org/apache/commons/httpclient/methods/multipart/PK.....eW.7.....%...org/apache/commons/httpclient/params/PK.....eW.7.....'...org/apa che/commons/httpclient/protocol/PK.....eW.7.....#...org/a

C:\Program Files (x86)\PWMinder\app\commons-io-2.11.0.jar	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	327135
Entropy (8bit):	7.923604489259355
Encrypted:	false
SSDEEP:	6144:UrBoCnU0+1j/OjXrf50ynaZ13lybiOmQ+CEEArHs2M1mX2TKYGGh82ajQe+yw:2oCnU0+hnZLOm7CH4Hs5mXmKYGer3
MD5:	3B4B7CCFAECEEAC240B804839EE1A1CA
SHA1:	A2503F302B11EBDE7EBC3DF41DAEBE0E4EEA3689
SHA-256:	961B2F6D87DBACC5D54ABF45AB7A6E2495F89B75598962D8C723CEA9BC210908
SHA-512:	5BD78EED456EDE30119319C5BED8E3E4C443B6FD7BDB3A7A5686647BD83094D0C3E2832A7575CFB60E4EF25F08106B93476939D3ADCFECF5533CC030B3039E 10
Malicious:	false
Preview:	PK.....Hy6Pk.a).....META-INF/MANIFEST.MF.U.n.@.}...X.P%.^c.i....%...(./..VY.{.I..c..-...I.9s9..H>g....6\...p...i&X.%....[.:..#t.PO.....|...D...3T....S..A..3M....X9..[0.. {..f..X.H..^x..`...,...UiF4.....,.h".\....Kb"..:.D.....*..`.....I..*...H..2u.UU.S&....f.....j...P..&..z.....&..L..d..5..hP....h.1..n.e..^.'jnWD3.. |..Ld....P68....._.....Ju...m...B./.m.6E.t,.*c: ..V.u..H*\..f...2...w.`..... D.@w{...*..09;.E..3..d...I.rCo5.....*...f~*..t....k...k....Y1.0.f.1c..dw.../.k[....I.....e...J...e....q.[..8..[.'CS....r?}.n7.4".....B.,..g.|.g...SN.68.....=.../%w;.. y.c9Is=...y..e.I...8...<O.x.5. .!.x..p....'.s.l\j.n..D.?.N.....~*w...w.....I.....?.m.....$....F.IT..g..\./..n..PK.....Hy6P.....META-INF/PK.....Hy6P.....org/PK.....Hy6P .....org/apache/PK.....Hy6P.....org/apache/commons/PK.....Hy6P.....org/apache/commons/io/PK.....Hy6P.....!...o

C:\Program Files (x86)\PWMinder\app\commons-lang3-3.12.0.jar	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	587402
Entropy (8bit):	7.928552551034422
Encrypted:	false
SSDEEP:	12288:+ckjxCcwZ/O05RmbNxmLhmckii9z2B19dCk:ACcEOqENQEvUBlF
MD5:	19FE50567358922BDAD277959EA69545
SHA1:	C6842C86792FF03B9F1D1FE2AAB8DC23AA6C6F0E
SHA-256:	D919D904486C037F8D193412DA0C92E22A9FA24230B9D67A57855C5C31C7E94E
SHA-512:	FBDBC0943CB3498B0148E86A39B773F97C8E6013740F72DBC727FAEABEA402073E2CC8C4D68198E5FC6B08A13B7700236292E99D4785F2C9989F2E5FAC11FD8 1
Malicious:	false

Preview:	PK.....Hy6P9.....META-INF/MANIFEST.MF.UMo.0..G...8.....T.Z.JT.V..q&.....$@..m.F.yo....*y..z.@..d.4.....D@..R...[.-r.P6..Qq..!}*..s..P.....<.9..*..O_.....#.S.Z..].&.. .c..Hib.....vF-.....A.@....8h..lU%.....XE&@.".X*C.CBMv.....%7.$....]jU...7Pa..4F.JO}....ZW.h...9.i0rfmbZ..b..".\..{S..:.....~.K[..V.Da.w.v.St..7..y....8.^.P.....Td..e..3. aX...>5.E#.B....E.:....7..*...).....>...*,.h....x..Z.?VTO2...=.Q.fX.;..z.....5....Z\o....P.>]....\...r'..c.....t.]9.q.9kg.>.....y.u.J.....8.hu...A.qu...l.....~k.....zn*.r$J....S...!|.r...v. <G..+A5.. .g .R....C.]./.{5'..9.....A..w1...,J%;.. O...uJ.....H.....'.f.y...mai}..4...(!..X....R8..i".!.Z/.....z.N...o\...Y...U.6.8.d.B.D:.r..].u..PK.....Hy6P.....META- INF/PK.....Hy6P.....org/PK.....Hy6P.....org/apache/PK.....Hy6P.....org/apache/commons/PK.....Hy6P.....org/apache/commons/lang3/PK. .....Hy6P.

C:\Program Files (x86)\PWMinder\app\commons-logging-1.2.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=store
Category:	dropped
Size (bytes):	61829
Entropy (8bit):	7.924448014410102
Encrypted:	false
SSDEEP:	1536:TWvDr5xeO4G9Q7+VCfSqguGukQYvFABhbHoneHz:6BxeO4CQSoRglukQTrjoeHz
MD5:	040B4B4D8EAC886F6B4A2A3BD2F31B00
SHA1:	4BFC12ADFE4842BF07B657F0369C4CB522955686
SHA-256:	DADDEA1EA0BE0F56978AB3006B8AC92834AFEEFBD9B7E4E6316FCA57DF0FA636
SHA-512:	ED00DBFABD9AE00EFA26DD400983601D076FE36408B7D6520084B447E5D1FA527CE65BD6AFDCB58506C3A808323D28E88F26CB99C6F5DB9FF64F6525ECDFA 57
Malicious:	false
Preview:	PK.....|..D.....META-INF/PK.....{..D' F.....META-INF/MANIFEST.MF.T.o.@..N.....A..Zk.[.M..K....[.].,b.....m{...2...}.#"...?S.2)|.X.i..T.?.`|".#.".$$XP+.q,Ejq.ELD.. .....^.i..\.....M4|.S.9...9PoS..7..q.1.....0....GW"...-.v:...c.u].....P*.M...0.s..E..DX.}...9..$4`s.\|S..9.C.P.B.B..o..<.....\|.N..A.?.../..k..O..W.Yc...XL.....j\|w}_...I{..w.....*y.Y_..(.4,... ....h.F.<....T@..:..x...e.?..Y.....<_.hHR=.!.O.....3..95nT..._..i.X...O.....L ..DS...2/B./..s.e...<^..K..H..U-...r..B..U....T.8.j!2..4.lk....%....\1.Ks...Y...R..T.....V..i.8:W4.<+...0.hE. ....p).....R-K.R...*....x.....7..*./....S...G.Mu[..=.p...x.R....>....x0.i.....^..]...2.z..?n]s#...4..$.k...v0..93w..s.)..>...s.W....lw..w..*z.O...*X0.....:K.6`....PK.....z..D.....org/ PK.....z..D.....org/apache/PK.....z..D.....org/apache/commons/PK.....z..D.....org/apache/commons/logging/PK.....z..D..... ...o

C:\Program Files (x86)\PWMinder\app\custom-components-2.0.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	23470
Entropy (8bit):	7.6030979267967815
Encrypted:	false
SSDEEP:	384:f0fevVzwTXkj5r1fM8712YVIayjbMGS40lTogup6i7O8rpIJ+iV7hYnD:aKVBpei2YV5XlcbpEg2slhcD
MD5:	84F46F40503F335D3953F87387EC8162
SHA1:	001B49ED5DE13C651C8DCD3CC8AF3DB17AF6E863
SHA-256:	0B22A5A3A9E8F54BA71A59DF04E162C976BFF084E40400AB4BBFD51437255B6E
SHA-512:	B7D943959500F28E001BECE65E9E202609B0D24D57E0AD9235031707165EB2D04799119BCD23891242014274CCE2F0516C052E88FFC8469A3BF91FF4946C4744
Malicious:	false
Preview:	PK.....xo.T.....META-INF/..PK.....xo.T.1.!.....META-INF/MANIFEST.MFe.O..0.G.~...MH.]....4S...^.....L.?...C.I...B...w.<.4H#.-:...F.....E.y....m..GVC..... $..`\|G_R)..\Uu1.e..(UE.$.....u_.i...(..]{.x.....-/.c.sB.i...O6....8.<..PK.....^.T.....ca/..PK.....^.T.....ca/ewert/..PK.....^.T.....ca/ewert/customComponen ts/..PK.....^.T.....".ca/ewert/customComponents/buttons/..PK.....^.TW.mK.....5...ca/ewert/customComponents/buttons/ButtonFactory.class..[S.U.....,0... 1...m..#A@4Y.!...A..d.&.lvg..Y.T.....-.}./@...X.Z.|.....%.....nf.5TN.....}..._.8....0..i.....0/....X.qN..e..rI...d.....\.qQ.Wd...k2^Wp..#..tbM.3.}=.S..[<.ziv.....k.....-;>&.>...W.. .=..q....U=.+..1g...9.6...53...%L..1....:...W....s...7.....$cN2...f....2.v...:.[.h0..g}.....q...z..Z..W...3.m=I.:.q..Vj..J.....me../..q}^O.*..).....a&.aU.h..I8.3..3v....S7-7.R.].F.jf..[.y.i.N^!.NI.

C:\Program Files (x86)\PWMinder\app\dropbox-core-sdk-5.4.4.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	8027912
Entropy (8bit):	7.922213819507639
Encrypted:	false
SSDEEP:	98304:i6cvpRcVL+kozLUQKzyA2BZB0aoCLCa8kOGbmZ1MMrT2MCKirjp:PUpRq6wdy5BZuBE8kL49rqdJrV
MD5:	245C7EF06C51700DA9C46B9974B2A2EF
SHA1:	9BEA02CD9388B3B3E084CD9A919A8937ABFA02EB
SHA-256:	BE5D859649F08C58E0D8B724A5BCEBF561C343ADF01D5227BFD1493B7D599E7B
SHA-512:	EA9716EB105A07B738F6B8DC4890F3FA14E15EC4EA1FEFF327305E93F8EC38FE1AAF745F0F1FCBC99DE45F7CEE2F5E92DF0FB210A8783069616F2F15B6E2757 B
Malicious:	false

Preview:	PK.....uQU.....META-INF/..PK.....uQU..\8.....META-INF/MANIFEST.MF.YKo.8.....zX.@.&i..M..v0.....v0.9.....%.%....%....l.{j*R.)..H..K.Yh3..b.+..,.|<.K.6....Z.....Xp#...#..3[.&...J...Q.....^z.b<..T.....-.q9_.....r>.....k.../...Z..O....W....H.f....|'..O.l...I.1O.bs..=.a...l.h..gM..h.^...M.{.J.W.QR.....R.&...'.$x<.....A...A.a..3.C.oa.^q..).....">...9....Ri\...Y%'3.E.....R.....U. 1a).H9..h...Tj..2./.?...V~.f@J...R.":...z...O...E[..xi.z.D9,.Zf..R.@.....%..Y....x.....E.H.S...3..[cZ..l.....P.C.....K'.ho.J...]..WBG.....i....Z.g.....E..".. ....HDY..s..s...)M+.u.. ..: Y.1..k$K.S.D.D.....i.)..l.p.....r.....El|.N..K,~&....0?.<.n...=(R.AIA.....}.#7..C+!@/.....R..HC|.....4..N\(...#..->T.Z. YD..V.r.4D...H....Jv.....X..... .....y.H.Nq.C.^.V6.h*<....M.F...g..0._N.z....Y.P.....4.{.TL...>...[M+.~....n.....-..F....h....Q...ho....h..F.Bj..d_.&DaW.....]...2.....t.P....w.<.+O\FVE;,....!.3?`....$k)8$.Xr...5G..]. .....lucV..W.}

C:\Program Files (x86)\PWMinder\app\flatlaf-2.6.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	730429
Entropy (8bit):	7.958886340283549
Encrypted:	false
SSDEEP:	12288:TRcW2DgPL8+td5yiDq3rvnk5O7GdZvjzwrEvIDIH/8L:Tr2DYLx5gHGXjeIH/G
MD5:	8C4F71BF62708FA7881B82C62579824F
SHA1:	4DD2BA228E3C57EB3D80E3927B5A6A33265EB69B
SHA-256:	6A897CAC19C4F48B22884A21A7DDCBFA47C7FDA266DBA69804A6F847AB9E97C8
SHA-512:	C1F91EE24F93F86C2F4BCECDD200FE8C3CA00E8C79FE28A027F75F5C8B8425AB182E044C717FA1482542C21C1A98EA5B37F5FF9CDD97BB76D26591CA6D0159CB
Malicious:	false
Preview:	PK.....JRU.._.....com/formdev/flatlaf/FlatIntelliJLaf.properties.V.o.8.~._1..R+A.=...T..[v+8...}4.$..s.C...7..J(../....o....g.p...Yn.zt.+.+]Lq.+..i.?...sr\|.1J..T2A.6G..,.....P..$\G#.p.....v....@*..A...R...%.....6.a... ~6.jc.y3./.....{rk...y....P.G3|.....+?.@c@.?...f..$>1..K.jP.X..IV9.....P.n...v.j.Q..$.....`...d.....4_.].X....q.X.g+X>..r1.....a....i....0.Rj.Hr'#&N..b.@..!Sb.S.S^2.X...-jI.@.....P./.e.y...9....%.O.XB..x.{...Ka.-.....].0K.-..b...sm...%..... ".Y[.....T.<.y.S.W.....iz.]Hp.Q..S...,..ZQ.....].U=.j.W....CO`.\.n`.U<.-.4uz."mbE..}..F..j..4.k....k[s..`..U.i.x`..k.H+.6.../^?.Z...K|.Kc.%.0G.P.Oi....9E.r.....I&...:T.6.P.....e,.l..}..Y(}.U..n>....(*...f.w.s.P.<.}?.....i.Qg..F.....h...L.#.....P....y... ni.)..=.e...`..],.,]I...FT.M~y.{0.SG...t.[..E.....(.o.G./.&$m0.r..r.IRY...SV..3.H....'.e.-..... .-.J..C..D.C...._....U7A..{....M2...../^..4M....N6...>.E.....S.."w.w...>.....1

C:\Program Files (x86)\PWMinder\app\flatlaf-jide-oss-2.6.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	40748
Entropy (8bit):	7.92952400321866
Encrypted:	false
SSDEEP:	768:EOgK1MOQ/dapT4UyoUsb5J5/zdf+1MJrEVYXOt/x33BnclkkGDw:kKM0pT4SUsb5JpzVDJrEX3RnclSw
MD5:	342238D042F12709E30FC25D7EEF48A0
SHA1:	6F4D2197B9105A1917C2E0EB72E3EEA19FE90699
SHA-256:	711080466C977302AB3D9523F933CD25B753EA9547CFF114C88D0BEDFA6F8E4D
SHA-512:	6714E40762128A512F03810CBCE666A1DB792472DCF8FADB115BDFF5D55AE0BB76E984F8EC425476348E82007FC2B2A9B13A38A96C633D62A28D6C648ADE1311
Malicious:	false
Preview:	PK.....7JRU.....META-INF/..PK.....7JRU.).....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3....-.I.M.+I,...%.R....r]R.....J...R..s.<0T;..T.e.g.X).....F....F.FF.....RPp..Q..(V(J-N-*KM.....c...x.x..PK.....6JRU.....com/..PK.....6JRU.....com/formdev/..PK.....6JRU.....com/formdev/flatlaf/..PK.....6JRU.....com/formdev/flatlaf/jideoss/..PK.....6JRU.....com/formdev/flatlaf/jideoss/ui/..PK.....6JRU.....B...8...com/formdev/flatlaf/jideoss/ui/FlatJidePopupMenuUI.class.R]O.A.=C.v..".Z.T..(....45&..d5$....v.....,...O5....Q.;....{.~.s..._....Z..K...R.....x.W.}....>g.ll.0TwL_2.J....P.o.aL...D">..rq....*c..#3.....bac1../M..\...v).3I...:..u..(.....X....>*}.ww.01Zj..<WH..X...../4..l[.2..".i:..y..B.z../.?`.aD.m.>1.oL.F.....Y...i.....&..gx.....3<..Y".t3..FG.....ch....2...._T:."......:SFc.....).....3.f.....d....W..q.s%.)u.Z..f...n..." .Bw..M..0O...K.=T.....*..I

C:\Program Files (x86)\PWMinder\app\gson-2.9.1.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=store
Category:	dropped
Size (bytes):	265030
Entropy (8bit):	7.88140539884304
Encrypted:	false
SSDEEP:	6144:AsmEEHDY54UOu/ciFk0H4FCBEWLhFaDt8b2:TqH85Ou/cQkS4s++X8p
MD5:	0D507D266DCF7EEA4B53FC3778D901C9
SHA1:	02CC2131B98EBFB04E2B2C7DFB84431F4045096B
SHA-256:	378534E339E6E6D50B1736FB3ABB76F1C15D1BE3F4C13CEC6D536412E23DA603
SHA-512:	10BF91C79AB151B684834E3CA8BA7D7E19742A3EEB580BDE690FBA433F9FFFE3ABBD79ED3FE3F97986C3A2BADC4D14E28835A8EF89167B4B9CC6014242338769
Malicious:	false

Preview:	PK.....Is.T.....META-INF/PK.....Is.T.....META-INF/MANIFEST.MFUT...z..b.TQo.0.~.....a..8$h0.".ehj.]U....H.:vf;....@.].Y..}w..WT.-...6\....u.....,..#...b.w...zo,.f.]IF..sYq....c.....,XRcW*.[.....0.LF.hZ..L@0W.Rf/.L.1..`mi.0.}.6..".....Q.....i^..h...n<.7....M..w..X....4.x.EI...1..3..c..y....m.D.<.m...W...x.E.E..;..A.N.3....6:..~U\C.x.V.m..k%..6..b..L.....x=_%^...7....SR.....aE.c..&o.....?.`.B....0....K.:..y.....D..$:.....R.j!.iy....AfJ.....[.~bU...GPgp..s...n){.....g.....h....t86{0...S..].)..^./)....Z/s.L...2.K.o....<].8..T.....%.j...7.E^.>.i0.k.p.-~.....\X.[.C...{..p..}..R"..OcLF$".0....$.Ec.YU.r<...>L.+p....PK.....J.....PK.....Gs.T.....com/PK.....Gs.T.....com/google/PK.....Gs.T.....com/google/gson/PK.....Gs.T.....com/google/gson/stream/PK.....Gs.T.....com/google/gson/reflect/PK.....Gs.T.....com/google/gson/internal/PK.....Gs.T...

C:\Program Files (x86)\PWMinder\app\httpclient-4.5.13.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	780321
Entropy (8bit):	7.923180926731671
Encrypted:	false
SSDEEP:	12288:NmjM46szuytdXV3UaftwJEAV4+bcYroWxk11cg+p9OB3p:NUM4hHdF37VdA6qrookUBEp
MD5:	40D6B9075FBD28FA10292A45A0DB9457
SHA1:	E5F6CAE5CA7ECAAC1EC2827A9E2D65AE2869CADA
SHA-256:	6FE9026A566C6A5001608CF3FC32196641F6C1E5E1986D1037CCDBD5F31EF743
SHA-512:	3567739186E551F84CAD3E4B6B270C5B8B19ABA297675A96BCDFF3663FF7D20D188611D21F675FE5FF1BFD7D8CA31362070910D7B92AB1B699872A120AA6F08
Malicious:	false
Preview:	PK.....CQ...#.....META-INF/MANIFEST.MF...N. ...I..n...-1.mK.f..nzj.|]..i(.x...f..x..B8]B....F{.I.f..Im...".Mz...'.Z...6.zct:.h.FoSH....}.6%}82.Y.....Th..|q...-Y>.h.j...+.3p.h_...c.).89$..I...)....:...[.U&4.x.S7l...g....T.6.....I..:u.q.f.w.|...\..'N:X.e...H.....7PK.....#.....PK.....CQ.....META-INF/PK.....cCQ.....org/PK.....cCQ.....org/apache/PK.....cCQ.....org/apache/http/PK.....CQ.....org/apache/http/client/PK.....CQ.....org/apache/http/client/utils/PK.....CQ.....org/apache/http/client/entity/PK.....CQ.....org/apache/http/client/params/PK.....CQ.....org/apache/http/client/config/PK.....CQ..... ...org/apache/http/client/protocol/PK.....CQ.....org/apache/http/client/methods/PK.....CQ.....org/apache/http/cookie/PK.....CQ.....org/apache/http/cookie/params/PK

C:\Program Files (x86)\PWMinder\app\httpcore-4.4.15.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	328324
Entropy (8bit):	7.885864221238314
Encrypted:	false
SSDEEP:	6144:hgzgAHvaOAVKF/dB+bzfYMX/gmAjBBSF0Eo5FzepwR26cV3/5jtg:h87v5zFqbzQu/PA9Bc0EojepwR26Qm
MD5:	BE7C67929DF007FCAC6C8EFF5322D3A0
SHA1:	7F2E0C573EAA7A74BAC2E89B359E1F73D92A0A1D
SHA-256:	3CBAED088C499A10F96DDE58F39DC0E7985171ABD88138CA1655A872011BB142
SHA-512:	F0605E4D521C6E9C7E645905687C519239FA9E2128403A515E6118B0406B503B0865A8EAD197F8532186B0C9AAA4189FF5BB301D5B0CF84BD54FA2258D17551D
Malicious:	false
Preview:	PK.....%L.S....JM.....META-INF/MANIFEST.MF.R.O.0../....7..0...#(...7S....K.i.....Aph.....{.Q..P.....J&($..MDY..i..E.....S..(../.....T5..6J...g*...s*l...;.-.....km....l.....0x.n...|oQ..k..p.*.....Z..y....e..}....$=....c.Z..ry.n7g.....53vyqF.0.{.'.lp;.%...<..u[;?at3..:.....K..\y^.....(.a.....&v.(>..9.Z.Z38..k....J..3.....?...i...1...8:q.p.....&...PK.....JM.....PK.....%L.S.....META-INF/PK.....K.S.....org/PK.....K.S.....org/apache/PK.....L.S.....org/apache/http/PK.....L.S.....org/apache/http/util/PK.....L.S.....org/apache/http/ssl/PK.....L.S.....org/apache/http/entity/PK.....L.S.....org/apache/http/params/PK.....L.S.....org/apache/http/config/PK.....L.S.....org/apache/http/impl/PK.....L.S.....org/apache/http/impl/entity/PK.....L.S.....org/apache/http/impl/bootstrap/PK.....

C:\Program Files (x86)\PWMinder\app\jackson-core-2.7.9.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	253357
Entropy (8bit):	7.950280807436457
Encrypted:	false
SSDEEP:	6144:7NeFdocRIuHkb6iPZhTAJ9Jv7ralhkOpQt:IMQw6iQV7rnP
MD5:	F5D0DFE03814113D792E75E885699640
SHA1:	09B530CEC4FD2EB841AB8E79F19FC7CF0EC487B2
SHA-256:	BD90721420BB899A974ED09A107FEF42CA8CC7C8E055762F6C81576132E5BBC5
SHA-512:	09A6506F93E64D31852524B2A18078D580E2936565311B4BCC44696F1FC76CD1B652B57D287253A87577987ED745CF45A5A5D09A59734D0ABF1028DB0173EFDE
Malicious:	false
Preview:	PK.....KZDJ.....META-INF/MANIFEST.MF.....TMs.0..3...p.i$l.1.!.:....4.[G..(.-W....]cB1qh.d...>.].|...L*.B...(..C.....g.....j..1jm.....".V'=..qo!Mu...]...S..>....M.7%BD.JK.$.u..Tq....S...<...l.....g..!1.....ZG.T<...8".|..L.L...v..9....K...n..F.Y3".W....G..t>.Ub...'..h...)4.....R@...2.. s...(.$.....:],.....}...^<.n.&t.B....=.6.w.....*.n....D.>...e.C/.A..W09L..2.?l....@.<....z...d..... S.C..5O.....+..#..$.`.f..Ul...e....@Zp.....L. .".6S9...?..1....e...5..P.'.u..z....g.....yw...#...s..0...% .t!.o.dmVl.V..]7..a4.V....".x..D,.....dq6.C.*=..B..PK..B...<.....PK.....KZDJ.....META-INF/..PK.....PK.....DZDJ.....META-INF/LICENSEM.1o.1.....$...:.U.C...u..K|w..D..S.}.....9.B...r.;.G..v...@.Y@M...((J...H.T.O.()E.R$.....#....(.....$.5..?.rQ.....F..H.|R..O..k..&.z.....0.[....s.. 4..k.Z./h.s..z...g..]uO../x.G.87..M.....Z.....n.*...PK.....L...PK.....DZ

C:\Program Files (x86)\PWMinder\app\jasypt-1.9.3.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=store
Category:	dropped
Size (bytes):	142255
Entropy (8bit):	7.839312023506353
Encrypted:	false
SSDEEP:	3072:WQwW8A0DsuACgLNZEkUn3artlyOvgfWhZvxxtEe:WhYLNykQKXofWhhtV
MD5:	39327C7E38782102ECDB3C9DC4E8DCD3
SHA1:	0D99EF9540F51C617F2A293B460F025D2EE563DD
SHA-256:	F481FBB8DD8CE754BFDE7552AF4FCBE8C5E303D53663BB3D8CE9D4338E0E55AA
SHA-512:	99369DA44E4C26F64E600F99B135EB05167AE1EBB5BB9F22233F14023F5416318BB4CA5893DBB0E7D444395EA6FA53713559A6990120B4FC962A1E9284BA5821
Malicious:	false
Preview:	PK.....I..N.....META-INF/PK.....H..Ni|.by.....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3..r,J..,K-B...V..+.$x..J3sJt.*...J...K.R....J.sSy...R.KRS.....e.y. .zfz...).^). .-.....\.PK.....N.....org/PK.....N.....org/jasypt/PK.....N.....org/jasypt/encryption/PK.....N.....org/jasypt/encryption/pbe/PK. .....N.....!...org/jasypt/encryption/pbe/config/PK.....N.....org/jasypt/util/PK.....N.....org/jasypt/util/password/PK.....N.....!...org/jasyp t/util/password/rfc2307/PK.....N.....org/jasypt/util/digest/PK.....N.....org/jasypt/util/numeric/PK.....N.....org/jasypt/util/binary/PK.....N.. .....org/jasypt/util/text/PK.....N.....org/jasypt/normalization/PK.....N.....org/jasypt/commons/PK.....N.....org/jasypt/web/PK.....N.....

C:\Program Files (x86)\PWMinder\app\javax.activation-1.2.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=store
Category:	dropped
Size (bytes):	78030
Entropy (8bit):	7.917287230623689
Encrypted:	false
SSDEEP:	1536:k3VFP1b/A4TumsCfqU4MfdLzvi2qSfJ7CBqYkqG7tk7X:k3VFB44TkChvbqAJ+BqRqGBi
MD5:	BE7C430DF50B330CFFC4848A3ABEDBFB
SHA1:	BF744C1E2776ED1DE3C55C8DAC1057EC331EF744
SHA-256:	993302B16CD7056F21E779CC577D175A810BB4900EF73CD8FBF2B50F928BA9CE
SHA-512:	B4CBDD8FD1703E4B2E1E691DB78FBCF2232D836F740D1821C4C191A14F9472508E27A40D06E4B6B153964AF68032959C22945BA169A0CA4018B7748162F420A6
Malicious:	false
Preview:	PK.....&K.....META-INF/PK.....&K..LO.....META-INF/MANIFEST.MF.T]s.0.|.....S.6..:.. t&.H2..#d.Td..d0.>g....W.iowo.3".;3.{c.p%#...u&.Vi...!+.._dG2L..;b. ..5.D....IRyR.....3.q.t.+p.;!.v>...8.C.o..I.@.....0...H.v..d+X.=.z.nE.&...\Xot..Y.).O..D.F2.....^....X...hB.P..V%P..L.`.3I.i.a.0.c..R.....wN....h.4W..5.V..A{.7....%c.1.I..kk.&.....t.a...c. ..K..~B.e.>.'.....V..C.T..B`.N...d.8.jjW...R....i..%...2..$..kF,....q..?.n...,4V.N....>..p.$..87..S...{.7'.'0MQy..`5...1.@..n.7_{./.<r.Yy...nUz`.j.....R~..... ..G...k4.5wE.\....X..{.....\ y..h...q.....i.CM....h..e).U.\.u>.PK.....r&K.....javax/PK.....r&K.....javax/activation/PK.....r&K.....com/PK.....r&K.....com/sun/PK..... .r&K.....com/sun/activation/PK.....r&K.....com/sun/activation/viewers/PK.....r&K.....com/sun/activation/registries/PK.....r&K.....Y...%...java x/activation/FileDataSour

C:\Program Files (x86)\PWMinder\app\jaxen-1.1.6.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	231882
Entropy (8bit):	7.823455495820713
Encrypted:	false
SSDEEP:	6144:zoy/QchIyZukCzO/r+ASaZ0gJ+tbEZx+m:vDhIyDEOT+U0Fk
MD5:	A140517286B56EEA981E188DCC3A13F6
SHA1:	3F8C36D9A0578E8E98F030C662B69888B1430AC0
SHA-256:	5AC9C74BBB3964B34A886BA6B1B6C0B0DC3EBEEBC1DC4A44942A76634490B3EB
SHA-512:	6BD11529D6DFCB27DDD485C8DA2440D3686CB61693A9461833A2BED49407343DF4BA707F45164A6E69B78979581D91FBF0F6C5EAB28653DCFA724AFC8952977
Malicious:	false
Preview:	PK.....=-B.....META-INF/MANIFEST.MF.....VM..0..#.?X....IQ.....B.v.[e.C.:v.;|..w.....yo.<.!.....(&...x...D0Z..72`{F.0...b:....^. e<.=..&..O...Q...=DyH.i,".t..*?a....HF.b.... v.]..x"....Qq`..:X.....I..L..f.|*..@G..m.....Wq.....O...../'.I?.....L<.X.Z....*g.P.i...KL....9AK.<.....e.L.hK.Wr.9(..u.Dk..e...V.....I.....q..H.4!.).!..g.<....y.C..Z.;.h+.....%...+0\.S? M&.s.H.W[.....6..1....+...L.v.C..r.....w..>.\9.!..0..0}..}*|.Xq..n..S.....V.7fW.@.V.-.b.?..MH.....rV..2.....#.j.t.~../.n.kWw9.k.v.x.~.....u.[...,p..u..|..-w..&vGI.....gS]_).W...97 ..Lv.K..z.sy};.....{ty.[.]&TI..+.....'....Aw.}-Z.3.3(.|.....~.....S.K'.....{..K.....c..PK...1ak.....PK.....=-B.....META-INF/..PK.....PK.....b..8.....META-IN F/LICENSE.txt.TOs.6...S...C7...n;mz...u..JrXzs.X.b..E...}....D.=....7W.|d.=.,.....Op7..x=.....w.....~...a.8....2{|q.....C;....v....._&@....o....t;I .....3.'ol.M..i.`z...mu.y4}.^`g

C:\Program Files (x86)\PWMinder\app\jdom2-2.0.6.1.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped

Size (bytes):	327806
Entropy (8bit):	7.9384244790428315
Encrypted:	false
SSDEEP:	6144:/PPwchREeQkgo4zu/6i8q58PPZh5oAYnjXfuPDZeISX3UG:/P4OZQkAy/M1ZiCL6F
MD5:	5BE72710C66F3C9BA71F8009E92597D1
SHA1:	DC15DFF8F701B227EE523EEB7A17F77C10EAFE2F
SHA-256:	0B20F45E3A0FD8F0D12CDC5316B06776E902B1365DB00118876F9175C60F302C
SHA-512:	81642DB76358FBF131DFE9C2F1D9C280FC23B6BFDE6A16A2D36DACC490A1A2AF4E0FB4ABB5CD78005718BB1D158A42FD6834CD2BFE616EC59625DF01951F278
Malicious:	false
Preview:	PK.....p.S.....META-INF/....PK.....p.S5..!@...Z.....META-INF/MANIFEST.MF..AO.0...$.....%Y].!.dM..7fo.Bqk.m....R..Y...y..^s.YM../Ti&x.0.. ..%..<P`5;.A.*.2E.....1\|.1.(.)..2..P..K.....IK. .;..D..A....I.0x..d5+]..1.X..]...!ZS=...c....)..J@...0...-...I..a...q.c..6._.x..{....q.E.m....s.91r}<p....^8...FC!..."...E.t0..?u._..nZ..w._.C!..F..k..E....F..0v.p..$.x...u.Bwu....PK.....@.hS.....org/PK.....B.hS.....org/jdom2/PK.....A.hS{..?....'.....org/jdom2/Attribute.class.9.xT....N&7..H....!.$.PP..!....@..r3.I.'3q.....W..Z./..(..$.....Gw...lk....u[.u.....;7.....y.....[.~.%.X..z.....T....x._/...?3....< .J....!7!c...Qe.b...^(.B/jX.b..K.0.Ky....}.....8....X..N.,.*x..s<8..L8..._..^X.....{p!.8..<x....%.D.*Vh)..x1..*....^X....Wz../...xX....p....9.\....}.....b..<...n..y....F..{.....Y..Tl.B;^...1...k.b+..j.y.b.l..;q..[...>.B...y.....a.{F..a.C!.z.2..c.....d.J."..2.e(...CW1.

C:\Program Files (x86)\PWMinder\app\jgoodies-common-1.8.1.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	37807
Entropy (8bit):	7.758178243971047
Encrypted:	false
SSDEEP:	768:p3NBXFU4rm5fkbJvenfzm+R6h9i4Y+hsfqRzQmBq0v:pvX+4u4vIRRQj/RH
MD5:	7E6BC1CD169E4F78D9529AF34A876F00
SHA1:	DFFC159CF71BDE5DCBB65916305684F6B43D45B1
SHA-256:	DDCA10C16E1DC7A1B399C14580F0AAE23014851E57D224CB96C260E6D649D2AD
SHA-512:	C51F07B79CF11CA34E5B5140BCED5AC6F50A923C85C875D31AE576C7FB2D64FD7A845609CBA20E87016F15803AC841C8A24DE433F59E200C11DB5149DC39368
Malicious:	false
Preview:	PK.....x#F.....META-INF/....PK.....x#Fx.....META-INF/MANIFEST.MF.....0.E....,u..T..]u..QP.Jl..h..F.7..U..s.3..F..x.G.(kR...$3oIV.....0.E1%...c...;?..a.....Cg.d^!L....>.]J.gU.....h(...R....0....Ba.t...l3.....).{.....8k.....u].F.....5..We$."a\0.....(M.3)..PK.....|w#F.....com/PK.....|w#F.....com/jgoodies/PK.....|w#F.....com/jgoodies/common/PK.....|w#F.....com/jgoodies/common/base/PK.....|w#F.....com/jgoodies/common/bean/PK.....|w#F.....com/jgoodies/common/collect/PK.....|w#F.....com/jgoodies/common/display/PK.....|w#F.....com/jgoodies/common/format/PK.....|w#F.....com/jgoodies/common/internal/PK.....|w#F.....com/jgoodies/common/swing/PK.....|w#Fk?.....&...com/jgoodies/common/base/Objects.class.T[W.W..N2.a..U..j[.....@.J.V4.kRl.i...`2.N&....?../>..Y.....k..|qu.. .`.V....}=.....0.M...V....U$5(X..m.,

C:\Program Files (x86)\PWMinder\app\jgoodies-looks-2.7.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	400791
Entropy (8bit):	7.888494042694628
Encrypted:	false
SSDEEP:	6144:I7CVxez0YiDb318jWT3+0Yv2TN10Rq38i0D2vA5rOi5N:IOVxezibllbWv2TtMHyvtON
MD5:	F6F746EE51C49A2D91E30BDFC8043443
SHA1:	7679705B2D03626740713898361 1A4DD3EC9B72C
SHA-256:	D7DFB4D041C28EAE836AA0910C91C1B95B29C28E833200D2EF6D311FA66B4C6D
SHA-512:	FBDA0C1CC3D6895F98FA6DEA00E67020D88BD411D9C2B9F5118AFF85A1F666ED5E885E28D322AEC19A87E53BB0FF9C541E2EDB741C0C1C06C1421056D8C6564
Malicious:	false
Preview:	PK.....Ox#F.....META-INF/....PK.....Nx#F.M.....META-INF/MANIFEST.MF...j.@.....s.....Vin1..m..x-k2.K....".}S.....?..?3o...C.;....@%....$yo.O.!.....h".b~..g...i.W....M."..{.&....."..6=V.....[.[.`U.....}...K...k;t5..oCM<..Pv.....)g.o.C...`D.W8...@K.$..2..fRg*.oPK.....Hx#F.....com/PK.....Hx#F.....com/jgoodies/PK.....Ix#F.....com/jgoodies/looks/PK.....Jx#F.....com/jgoodies/looks/common/PK.....Jx#F.....com/jgoodies/looks/plastic/PK.....Jx#F.....!..com/jgoodies/looks/plastic/icons/PK.....Jx#F.....'...com/jgoodies/looks/plastic/icons/32x32/PK.....Jx#F.....'...com/jgoodies/looks/plastic/icons/48x48/PK.....Ix#F.....!...com/jgoodies/looks/plastic/theme/PK.....Jx#F.....com/jgoodies/looks/windows/PK.....Jx#F.....!...com/jgoodies/looks/windows/icons/PK.....Jx#F.....$...com/jgoodies/looks/windows/icons/xp/PK.....

C:\Program Files (x86)\PWMinder\app\jide-oss-3.7.12.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	2126936
Entropy (8bit):	7.942775062184331

Encrypted:	false
SSDEEP:	49152:vPPLfCqIaHCBtqICLynX7xZmVecggpwFR9:vhMzqVWntZmVfggpSR9
MD5:	DF5B14FC6E71FD1D925DAB22AA720E61
SHA1:	D2909BECA24844D0E073226C8C9732C5F39A2B5F
SHA-256:	C22DA104E865657FEE24A8EF739A4827545C73132DCF3D584E9551D80DFBD82F
SHA-512:	238842E899714A217E60E5088F09BA218E23D214A4FA36B16958E901730F1B0F3E8F81166D88C686062D73050DD7ED4AC017D9B1B20A0B8F38AD963E00356820
Malicious:	false
Preview:	PK.....U..R.....META-INF/..PK.....U..R..,@F...N.....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3....-.I.M.+I,..$.....x.|KsJ2u.RsR..S..J.JSy.x..PK.....S..R.....com/..PK.....T..R.....com/jidesoft/..PK.....R..R.....com/jidesoft/range/..PK.....R..R.....-...com/jidesoft/range/AbstractNumericRange.class..OK.0.....ju..MO:.....=..WvO.8S.V.T.cy.<...P.....x.<y...y.x}.p.....-.....@.R....h.`^.3.0.d!..E"T...7*S.O..u.-..^..FQZ..L.....\x..R+.j..%..Z..v.....xUH..~H..D...+E...4..#.r.x7I&R..![,{RV*.W..d.W.5.....2..7.y..}G..m.S.Qw..@.....E..K.!.r.L.....R...l4q..&o}.PK.....R..R.7k....-...(...com/jidesoft/range/CategoryRange$1.class.T[O.A..fw..H.E.F.Eze)....4...$..DMt)kY\v.....b.....?.G..R1M.s.|..3...|.....G.#.. .:rCP..N!.Y.:.t.u.3..m'L.1$+....q.....Y.....-...x._f.N..g..Z...F*.g..v7.fm..3V...[..G..MM.a0V<.....6....RE.6q.q.....=+ k&].>X.K..g.;v./...YaPxQ0...C.R*%,..N.U.8^SF.....Z...

C:\Program Files (x86)\PWMinder\app\jnr-11.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	510926
Entropy (8bit):	7.9274020095373485
Encrypted:	false
SSDEEP:	6144:pt7EiKisTet9StvA0imDUuH1saxYc6k81/qMZitrbntDNFBZf2FGRYnzfdVi9GJf:PEiurtvY/ax38HiRBBvUzfLHxELCGzuV
MD5:	CC98F540F89DDFEBE6C62A7ACB9290DD
SHA1:	F31579BDC6535D7BA6004F503AB08DA8D1FC874E
SHA-256:	2108C31568860783F13097449356DA945504B92A62AFCE2198558094B5B9659E
SHA-512:	DA417A9FC03F58224A7521E2C6DB17E4ED945A325662F4ABC7A8D008DBA3C5ECD621C472385B0737B3C5CE68A7C3BFE5AED4F01A69B08FC885DC6484C0D15E1
Malicious:	false
Preview:	PK.....e.'S.....META-INF/....PK.....d.'SO..LX...d.....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3..r.C.q,HL.HU...%...,x...R.KRSt.*.....-.4....sR.....K..5y.x..PK.....`.'S.....org/PK.....`.'S.....org/violetlib/PK.....`.'S.....org/violetlib/geom/PK.....`.'S.....org/violetlib/jnr/PK.....e.'S.....org/violetlib/jnr/aqua/PK.....`.'S.....org/violetlib/jnr/aqua/coreui/PK.....`.'S.....org/violetlib/jnr/aqua/impl/PK.....`.'S.....org/violetlib/jnr/aqua/jrs/PK.....e.'S.....org/violetlib/jnr/impl/PK.....`.'S.....org/violetlib/jnr/impl/jrs/PK.....`.'SV.).....L...1...org/violetlib/geom/ExpandableEllipseOutline.class}R.n.P.=w@.x...T...H)j.4&....I..If..E...k.-I{...&..M|....}..5.mn..N.9..~.....O.$..$t$%R..*..k.U...v.....w.....s..@..f.FFGV...@..;....I..h..U.k..g\]..s.:Q.....23Z.U.^.E.....P.(...c;',.p....Hv..C..M..Xe..GL..

C:\Program Files (x86)\PWMinder\app\log4j-api-2.19.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	317566
Entropy (8bit):	7.908322270636156
Encrypted:	false
SSDEEP:	6144:2PtlX2DwtInh3m2mobY0y9EL4Zmy1DVHoFg2r6bCu1VOWarmXLR9SfaLqsSDNb8c:OlX23fmobp4ZfRighDO+LR9sNxIE5q2
MD5:	A7F8FC9751CDAA237A1E18059B4887DA
SHA1:	EA1B37F38C327596B216542BC636CFDC0B8036FA
SHA-256:	5CCB24AD9F92E768D0BC456D3061A737951262DF803E004D2CAD096B75A88D60
SHA-512:	F7CF3647ED90DE7FDEF377E4321AA9B9EA2512A46D99109B359F7FC5DCFE6D3AE9F879C212707EA4FD16D358D10D21C56D5178EC4803504745DE6FE48C66C37
Malicious:	false
Preview:	PK.....R-U..|GH...2.....META-INF/MANIFEST.MF.V.o.0.~G..@y.Z.8.d]BTi..M.j.i..&.....1M....$.$.t{.....e...0.y.C:.q.F..{.|.....k.....1.....ynO.....vI..g.".....9.....0dQ...Lc...,.p.....P....A57..>{Y.q%..1M.D.I. .]..w;.Aw..8.q9.9.!RT.&q.Q .}..k2.i.>....-S..fP+.j.^_..o..M`B#.....s.....n...D...k.?"K...S^...O.8...a...k.V%.,R #.j.?.$..%b...%L..Y..x.I.K..EK.!..+U.o..<.#.....[....tH..-.. .`...X...n.O.H.q..PB"x...;...Rn.7.'e..s.{.8S.Y.....u..X;..Ot::<XJCa..-..=..K..I.5L.b....74BC1bV2".F....I...D..vg.n.dz.:6R...@..y.k.:j..rP.dn<.o.UfD.=KU:...3.....sW5...U.....8..^.>....\.Y..m.Z.;.;..p....s.=.%]..$.....LaEz.+.D.....2Y.k.~....."2.@.$.7..A^>....e.g."d..1.T".'.|h(qM.L-.....I..RLV..+.L.Bp...M.....8.:.w..{...f7.7.F.....\.U.d.T.2.O.Y.N...Z...}..1C.-.!(.... ..H..k...2..W.c.G:..^o.&.MR....>..fh..9..q.m.....E....i..PK....|GH...2...PK.....R-U.....META-INF/PK.....R-U.....org/PK.....R-U.....

C:\Program Files (x86)\PWMinder\app\log4j-core-2.19.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	1864386
Entropy (8bit):	7.890502550882888
Encrypted:	false
SSDEEP:	49152:eCBdQ2xUbmi6TFTeI3EFRSd4r7Tcyb+NQ/QpJXpEfAD:eDuPA8c7YaU
MD5:	B7F521926226A16531F8E212B1DA1FFD

SHA1:	3B6EEB4DE4C49C0FE38A4EE27188FF5FEE44D0BB
SHA-256:	B4A1796FAB7BFC36DF015C1B4052459147997E8D215A7199D71D05F9E747E4F4
SHA-512:	1300ADA6F86818EF4DCD17448A8965C1C6DD41EC414DE2B2A5BAFDF25D03C12100FA9E8F422D7B346F2984E5DFB3D599F8C1A971A6BCACA0CF938943D0636 E7
Malicious:	false
Preview:	PK.....;R-U..J#&....O.....META-INF/MANIFEST.MF.\[o..~70.a..".<.g<..c.hn-....8[..B.8.II...K.}.!..).*.(..gD~"....."*.-...?hY.....dv.).....1-*.....].9>~xx ....P....L<...~....O..9!.c...|....- ....t.3v}.....ez]..?*Z.I.5.....+..Y.x..=._.d.5.....&...OO..._.V.....|...uT..a.E.....)..:...C.|.....F.....(.....]...G.....|.....G.-.I.7.}.Hn...^....K.<:}yx^.e..m....(;.YN.....8!*.&iD`X.D..,... [.!-...D.s[..DE...e.....=.. ..BNOC!....B..4(...q..C.NG*..Dut..I(...DW..H.8.N....."UmZ(.[:T.%M6`...3w.X.....`Y.....g..h...I.Fe.0.$...h...p...2.j.?{...y.=.S(...H*A+..8...>E....4...&iU6.... T.....IR....q_z.a.N..]...J}1....YCv%.iU.?k.....,.O.....0.....Y..s....b4..p^..8\ N"i..+h...}....ky.:....D.,..4.../RU.*.SnW...uOj....Eo...../U].(.~@.2**.L.....(K...#)J..=.YQ...w....V...jif ..YB.B"....>#....W..,...n...F...Y...P..&..n...p...p.....A....<...w.;....F.+....K.P.55`..x..2.c...p..5.2.`.&VOEl..8.0.-..k.b...+."..~4./.+..q.....g0.=..P.Y...

C:\Program Files (x86)\PWMinder\app\miglayout-core-11.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	105405
Entropy (8bit):	7.9685488108378575
Encrypted:	false
SSDEEP:	3072:LpqWnb3aDirStl5SPtrTX7NFnZpAar6jIliK:LcWnbKDiOAVTZpX2jGiK
MD5:	F0FA213B9170E80B1A5DFD09AF0CAE3F
SHA1:	99ECF243C6A64A038A568DBF8421928DB9B5C3B2
SHA-256:	812B9C8A8F326098A43EB9550229DD31100C49F81680EECDF6649DA423F0BE9F
SHA-512:	092CF82B095E619E96244E3B114F985C6854332C779F14C78AD1AB61CA85C2C2139E29851947492FD71DEAC522E6FA721FC5717B17DD8F9F98E417B1D25CC15
Malicious:	false
Preview:	PK.....K.R.....META-INF/MANIFEST.MF....MQ]O.0.}_....`.e.H.....0C..^..qkg..{;.....\h<.....C.3.Y.Gk....sF.j!?.....J .)P...R...Ew5. ...n..Qx@P...y:.O.|...Q.g..../i.....N Z..e...7.I.O(...).[i...d.....|z_g...tb..(43..W..x..+;^..E.=...UTp.....pw..&.u$i*Va.m..-.....XO.B~."h5.V..`Z..cq.d.A'....|7h..E-.X....W .X.B.`..`x7.b..q.....(..Sf...{..I.4If|..d.Gq..PK..j ..R.....PK.....K.R.....META-INF/PK.....K.R.....net/PK.....K.R.....net/miginfocom/PK.....K.R.....net/miginfocom/layout/PK.....K.R..... .....META-INF/maven/PK.....K.R.....META-INF/maven/com.miglayout/PK.....K.R.....,...META-INF/maven/com.miglayout/miglayout-core/PK.....K.R..... .....net/miginfocom/layout/AC.class.XyX\....7..f.`.@..$D..f.X..CB$....+J....x!/.f..`..Z...nim].....I....R..Z.Y.m.._...j.z...a...o...s..;.{.<..#..\....!.....E.n..g=...7.....y~|...~...._..!~|..._a. [..Un}-..r.6.

C:\Program Files (x86)\PWMinder\app\miglayout-swing-11.0.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	22899
Entropy (8bit):	7.8902564137646864
Encrypted:	false
SSDEEP:	384:E/Ck4YPzn5h2kGhBMZB5ZyScett1lBkGKb4P/mdHykhrO30sM3:E6YT5X2BMZB5ZRprCboMXhr3f3
MD5:	178B0CF219E824DD7BFFF4F63B838557
SHA1:	EA244BE3C4A16C541413C4FEBDEE539B348C744B
SHA-256:	7AA9DA079E0ED628A3672F8DDD1B6B05A5A3EC27639F82370956748943989BA6
SHA-512:	6C6672C5C2F3F6B6701AC1D6117F0E72966AB88CB7F28468E85F0C9AD8EDB74A6DA311D15F68B9815AC108C3D03CBF19EEF6E80564BD34F74806DDFD035DC4 BC
Malicious:	false
Preview:	PK.....K.R.....META-INF/MANIFEST.MF....]R.n.0..#..V.U"...&R...t..TaT5.nfe....I.6y...!...>>..d\b..F...*..F.0x..-.h}L...o@2..I..5..P....ZDO.#.P81s.....).%.p..'w..8Nn.W ".1e=dOi....>&.....`.....,....qr>e\..4).&.=..".`..@J.m..I..S.9rI..f..b..A.w.e.R..$..._...Q...c.+.....f.._.o.5.xh...3/>..D..b...>'..c....].0Z.g..%W..v..?...k...M..i...=.,...3.....4...gMY 2qi/.C...oy.5Z.Qe*.....|3>c+....d.i.....V.N...'..8^.E...0...PK..q.d.....PK.....K.R.....META-INF/PK.....K.R.....net/PK.....K.R.....net/miginfocom/PK .....K.R.....net/miginfocom/swing/PK.....K.R.....META-INF/maven/PK.....K.R.....META-INF/maven/com.miglayout/PK.....K.R.....-...META- INF/maven/com.miglayout/miglayout-swing/PK.....K.R.....&...net/miginfocom/swing/MigLayout$1.class.S[o.A.....E...Mi.a...M.@5jj...#.....h.G..|6...`.....1.]Q.4. 3s.9.w.s.....q1.....qB.I.a.=..#.

C:\Program Files (x86)\PWMinder\app\not-going-to-be-commons-ssl-0.3.20.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=store
Category:	dropped
Size (bytes):	190116
Entropy (8bit):	7.943718157296125
Encrypted:	false
SSDEEP:	3072:MhRE3Ha0oHX70kPlOdCStQwFqepYg5WsZPfCguzUEnLD/DY7kw006/slFNJONkIQ:MUaN70MStQwig59ZPfCNnH87E0zENkxB
MD5:	327A7CCFCBF2D5BD032634B8BDEAA83A
SHA1:	7502C294B7FEA7ABBD171A7DF15FED3BDB1E368C
SHA-256:	0E748E762AAB3FC692BBAC984633668FF28C17CAB0671F0425F85DE81819C34D
SHA-512:	59EB42519C3F7EF2B4CB18242222752254D99676304EDEC8596F03B3C1D534C5D1F70EA4E3B4F400BA027CF9F82D14BFA4B82245CBBB51338D969239F36CC1C

Malicious:	false
Preview:	PK.....|IIN.....META-INF/PK.....|IIN.....META-INF/MANIFEST.MFe..N.0.E.....q.".....j...-r.ib..T..1A...s..w..=a&x.m.J4....O.=..T .,9T.9.<D..8D..6...2...._-[yW*... .._yq.9g.+p....tW%.5..6.5a.....b./.D+.e....?..^...Y57K.^.J.DSVU5X..4.WA....U(....E8"...g"C.3..PK.....o....&...PK.....sIIN.....org/PK.....sIIN.....org/apache/PK... .....sIIN.....org/apache/commons/PK.....sIIN.....org/apache/commons/ssl/PK.....sIIN.....org/apache/commons/ssl/util/PK.....sIIN.....org/a pache/commons/ssl/rmi/PK.....sIIN.....org/apache/commons/httpclient/PK.....sIIN.....&...org/apache/commons/httpclient/contrib/PK.....sIIN.....*... org/apache/commons/httpclient/contrib/ssl/PK.....sIIN.....0...org/apache/commons/ssl/Version$CompileTime.class.W.[[....Hr..@.iik..p....[.....9=$'phr.....s...z...^.. ..Z....._.G..N....)..wy.....;...w/.."..p.Qp..2.RP

C:\Program Files (x86)\PWMinder\app\swingx-all-1.6.5-1.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Zip archive data, at least v1.0 to extract, compression method=store
Category:	dropped
Size (bytes):	1495328
Entropy (8bit):	7.908558330691433
Encrypted:	false
SSDEEP:	24576:2RRLsOfh9orWGa34oXRkUPvgZ4Ka4/uEy4+232LV3HGFAeLtixT:lwWkKhXuUHKO4GEybWClHIATV
MD5:	8F978C9184E5864EA90914052A781B1D
SHA1:	1EA704CD8779F8DF8A3D345EE1344239E7774D52
SHA-256:	2A4F82979CD16D8F1C9EEA232A985DFF62BF69C4794A37B96099B20D322907C0
SHA-512:	FF905482EF5041DDCBD3C496D2097A97027A367DABED0B6EAE3984B294360E910CD69BC67B5C300EFF97CE01D1443FAC4FF145AE006992BFFBD209AA1FDFF4 5F
Malicious:	false
Preview:	PK.....[B.....META-INF/PK.....[B.!D8i.....META-INF/MANIFEST.MF...n.0.....~.....[.M.d.j..m`,&.H.$.cO?)i...6@....Q.).^..-....6$.(./..d.....9.{..O.I.,.....l.G.i R...u|o..p..A./..[x(.}..&..x@a.:#yC..(.O$v.Y%...?.....S~....I...(.zW...1..s...g8.m.;C..R.M.3..t(....m.r0&M.p..Dpv...!..7.%I...''P\I.A..p\..@...wM..u(...].x..J.....Q.G....o.jo<....M.j.40r...4. .s...jg.,...Ps..@...;\|!<..c..Lh.X....x]...E\|...j...l.C..?\|jN.!.ss.]..'-{...2..j.W$..9.".A.*ao.W..t.k.>.....$.C.....%B....m.....E...F..\.-.h.....,.Q}...+&.....R.W..(.6t.-.....k.GjcH...&m..iv.. .;`.T.."X.V.x.....fz..r..:....o/1 ....:.m.F.f..... .'....tm...]#a..... .gI-...A`....+_v....PK.....[B.....META-INF/services/PK.....[B.....org/PK.....[B.....org/jdes ktop/PK.....[B.....org/jdesktop/beans/PK.....[B.....org/jdesktop/swingx/PK.....[B.....org/jdesktop/swingx/action/PK.....[

C:\Program Files (x86)\PWMinder\app\vappearances-3.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	32787
Entropy (8bit):	7.959128165950779
Encrypted:	false
SSDEEP:	768:Qv14S8Jp2GaaS0AXfvsEQ/xvXdC0Pri9onWCIM2:S+SZfUp/RdJri9oti
MD5:	0836FA7BB3668541FA31AF46356CF18F
SHA1:	1D3367522A1C8269489C8CB4E709E7BD75C83F78
SHA-256:	F8E5B21D63C35F70E431A118F446D04EA6524D9C6677E4A0389DC8CB72FD2BB1
SHA-512:	4BF8BF35CB3819794D125DF402AF14EE221D76564B5E0E3B2277A3E19D759A38E17860F3D14AB1614D603C489F83CD5904B563D5AFA2F770FEDFECAFA12B506 7
Malicious:	false
Preview:	PK.....s'S.....META-INF/....PK.....s'SO..LX...d.....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3..r.C.q,HL.HU...%...,x...R.KRSt.*.....-.4....sR.....K..5y.x..PK.. .....s'S.....org/PK.....s'S.....org/violetlib/PK.....s'S.....org/violetlib/vappearances/PK.....s'S.#.....$...org/violetlib/vappearances/BUILD.txt320 2.5..50.12.2..22...PK.....s'S. z&y.....org/violetlib/vappearances/NativeSupport.class.W.{.W.~'...LHX e.. l67/(.Aj..). ..@.N.C...Ygf...V[.V.xA)m...K.!.M,...EQ....<.....i \|..M.I...;g.w..]..~.\.....I..#.@..*..Q.p\...-..k..9n...jv....VP.h..#.....Zh...;.>n:..[.H.....1..f..f.L..vL.2O.i....m..P/~W[..^.C<....7...9...>b.!.U..z.;....z.9j.E;=....v$z...t..(....i.u4...p'. ...m..urvZ.I.Flb`.!..u].U..Q..P.q.Y...6....&<..(...U.E....C..4.....1.....`.....D.....<}.P.6Q&~.....b....?..9J.....]..{j....c.hUp.r.{r..6...!.U....fL..x..Y*..o...l'S.Pl.mk9 V...;"Hb.....Z.w..*R...o... .D..;.....?.Y.

C:\Program Files (x86)\PWMinder\app\vaqua-10.jar

Process:	C:\Windows\System32\msiexec.exe
File Type:	Java archive data (JAR)
Category:	dropped
Size (bytes):	2235078
Entropy (8bit):	7.947568556167778
Encrypted:	false
SSDEEP:	24576:VUdW7uNSLaHonVZmd6+xtRSBxzlx5hQ68c0brjfr2juwzXlmnzqgh7PhSkHELHF4:VqSuNOaIAOxzl1xE/KyIXtDh1HELlIlF
MD5:	B8C6865DFF79053CA7F510AD55B921E3
SHA1:	52A66177B7B03C81CF638EBDFA1F91BF5639C1A4
SHA-256:	7B86606C5F4C765B36328530BDD27F9C7996D0D2B76B566328510013CC787312
SHA-512:	949F86E7319F117BFCB70D49A7E4022F21E0CC855C51A8BB1BEBE792A3474351A909BF4480244D69B0B02FE84DBCD79D0A62E8BA22E0A73D85A2B9818A65B70 8
Malicious:	false

Preview:	PK.....t_-S.....META-INF/....PK.....s_-SO..LX...d.....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3..r.C.q,HL.HU...%...,x...R.KRSt.*.....-.4....sR.....K..5y.x..PK.. .....t_-S.....META-INF/maven/PK.....t_-S....."...META-INF/maven/com.sun.activation/PK.....t_-S.....3...META-INF/maven/com.sun.activation/javax.activ ation/PK.....t_-S.....com/PK.....t_-S.....com/sun/PK.....t_-S.....com/sun/activation/PK.....t_-S.....com/sun/activation/registries/PK.....t_- S.....com/sun/activation/viewers/PK.....t_-S.....javax/PK.....t_-S.....javax/activation/PK.....t_-S.....libVAquaRendering.dylib.dSYM/PK.....t_- S.....&...libVAquaRendering.dylib.dSYM/Contents/PK.....t_-S.....0...libVAquaRendering.dylib.dSYM/Contents/Resources/PK.....t_-S.....6...libVAqua Rendering.dylib.dSYM/Contents/Resources/DWARF/PK.....t_-S.....

C:\Program Files (x86)\PWMinder\runtime\bin\API-MS-Win-core-xstate-l2-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.672282124280155
Encrypted:	false
SSDEEP:	192:vn41usjf5bWWBhWSWYnO/VWQ4mWeZvmF4EHsqnajKse3pt:vn41usjf5bWWBhWIUbmF4UslGse3z
MD5:	DEFC34FAA61630DB1218170F389788AB
SHA1:	B6445CA0759B5D37D3341B4F760378BB17A09783
SHA-256:	044CC370D38456DE51D85AED25681AE40240DCB5CB2F809B681EF6FD1866B90B
SHA-512:	96C5B679FB39110094C759C6984D977F586592C918DF1BB2915936C19BC2912EA3048D0EF8F41F4C380FAFE7BC18A4F936538FFB2178E97756E9EA12F0391DDE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...@.T`.....!..... .....@.....~.....@.....`.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-console-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.612978494471077
Encrypted:	false
SSDEEP:	192:IlxoWBhWbWYnO/VWQ4mWdYgV5goqnajKs0Vc5:Il2WBhW7UY3V5nlGs0VW
MD5:	13FE5561EB3DB2CED126B79B79790799
SHA1:	384D673742AA451827F208DC05BECDF9958ACA85
SHA-256:	6BE5B5755C8C864096279FF311E3B0A77865E0AA7C6FFC6E6CE2622C789E43B1
SHA-512:	C388A50CE16C0798F43988FEB06B65B7D29B489CBA0A830CED1ACAEDB540B2D921F8D0416ACC6ADB7E3565EEED1D27062942ABC78873264A1A05E5DE495B2 94F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...Z*.....!..... .....@.....m.....@.....`...+.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-console-l1-2-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.6629297212483465
Encrypted:	false
SSDEEP:	192:PBuh8YWBhW3o2WYnO/VWQ4mW8OT2wNLrMhEqnajKsZ9WGjg:PBcWBhW3ocUCTVNjlGsZy
MD5:	CE582E3A15CB6776599A8AAE328831AD
SHA1:	71989C59B61A97C365AAD70DB69BBF6BDEE99552
SHA-256:	986A6C94776691DCC162D0AD49788C85E39BA255406CDDB42826FD98F12B4ECB
SHA-512:	6C27EF58B2DACB808FD818E69C058E6D1E3BF9C006D0887D3F0F2FE489852EACB49C25DA85444D84378FF4675AAE3859511C3460C1317CE6637E0C4B8AFC03(6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....+.....!..... .....@.....@.....`.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-datetime-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.621407370112907
Encrypted:	false
SSDEEP:	192:7+WBhWWnWYnO/VWQ4mW4hUj0j21EhqnajKs0qMl:7+WBhW0UmgqslGs0fl
MD5:	75D6DB7F779C887EE80962C18A411500
SHA1:	B76F21B4F8BC6D6F99F659CAF3A45E1C62E83B51
SHA-256:	51EAAAB1E5955DEDB71E27E77F8BAE0F960969487D115C53F38955ED7F34935F
SHA-512:	B9D902BB590DB08AD0D53410DEEA583EA77E74655CEB53A67DD0E74C0B358159C3E53CC0BDFB4838089BF5F8953499A45545E1F885134924D71B83026201E63
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...I..4.....!..... .....@.....p>....@.....`.....0.....!.....T..... .....text...p..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-debug-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.624124218922203
Encrypted:	false
SSDEEP:	192:wWBhWEWYnO/VWQ4mWdqq20j21EhqnajKs0qF4S:wWBhWyUZp0qslGs0aV
MD5:	FE7E3A0FE5CD4D960B208DB3F19F1945
SHA1:	13B5186FC3147DC9CC42648A265BD782E7BB6300
SHA-256:	6CE67FA67155EC601F42FEACD7FAF91A7DD9BD81070A5BCCF0BD12B4D8563B83
SHA-512:	D431D5E1982F02936234C7794FAF35530674305B3B8585AA0A3DECC4F0C598F19AD8597B018344D4E31BF9CC9F600771556EE388FF9037B6851F05BA2DDB91F1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...IGc.....!..... .....@.....*....@.....`.....0.....!.....T..... .....text...{..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-errorhandling-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.681604139827226
Encrypted:	false
SSDEEP:	192:jm1mxD3zWBhWWBWYnO/VWQ4mWAoi6dej21EhqnajKs0q9Cc:C1QWBhW4UsiweqslGs0oH
MD5:	91E6C1406BD499FF4B941D133D1898AF
SHA1:	4C9D0DAE41E235CD85C5665E42DBE92BE4FF9AB6
SHA-256:	BCCAD347EFCCC5E791929E30DC3ABAFAAB636CDCF23A7B68F3DEED016DD32083
SHA-512:	0E073DA892632DD1723FACF47A278422864E8E3CE4371A34AB2637999EA284E533ABF6B7BB321C6538BAD5B30C650ECBC56C48ADEA4C7BD2A030A182CD5B54 B0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....#.....!..... .....@.....w{....@.....`.....0.....!.....T..... .....text...&..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-fibers-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11744
Entropy (8bit):	6.6108542065001465
Encrypted:	false
SSDEEP:	192:dFhWBhWPWYnO/VWQ4SWdCbgIsmsqnajMtzGU:NWBhW/UhJs9lQtqU
MD5:	2ABB9BC8F00A5AD6EF2D6E4BE2B14ECF
SHA1:	51F1B7673FB63681809F8F69868A17076FF08C52
SHA-256:	D151BECE745A4749C3C117DB0DFB61CCB2E2742C72D9B0F1DB49E70EE0239DD3
SHA-512:	BF4D40E869EA83E9664F9AE96F72606AD94DA6C2A03CA59DC11D03EF1A661A4BE110098A1A3BA6AA1B61191F67BA3600E6BE93AEB41A38194A198FB18BFBB4 29
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...Z..y.....!..... .....@.....@.....`.....0.....!.....T..... .....text...H..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-file-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15312
Entropy (8bit):	6.575543244668128
Encrypted:	false
SSDEEP:	192:7SYPvVX8rFTsJWBhWDWYnO/VWQ4mWjx4iQj21EhqnajKs0qxm4:xPvVXbWBhWDUuQqslGs0H4
MD5:	070EFDCECB04C8CC7E1A8DED9A220940
SHA1:	5DF40DB56A5A60FB24E15D65A50780AE70200496
SHA-256:	A4C20AFE0F39CC27BBD55F98F94057CA8FD2BA72B920FE0F70F0742B26559D76
SHA-512:	34D5CDD4124BA0816D05282AF71A0AD6D082F8FCBE30A93707F167EB1B2E874147E85039DE3F387C7AAA1803140EC0AC338222850D9FEAA49DE131385358C0E A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....6p.....!.....0.....P.....@.....`.....@.....!.....T..... .....text...g..... ..`.data...@....0.....@....rsrc.....@.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-file-l1-2-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.649775485818372
Encrypted:	false
SSDEEP:	192:oWBhWcWYnO/VWQ4mWrjIsLrMhEqnajKsZ9LyNb:oWBhWKUUdjlGsZQd
MD5:	6E4AF6C8B50295CE9D2C7C89F6827334
SHA1:	86154197AE4765B638F884B47527C800C37D9CB8
SHA-256:	BE76CE72975A4E917325DB17410E50EC006BCD95432197370E601DC00E81444A
SHA-512:	C379D132A42B80DCB06C17A814E78BE1795AB8D07B15615AC268DB8FF5885E4BC7C46D1290CE23D162AC31A7801BD547CEACAB5048A57248C970CF78BF8C73 F7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....43.....!..... .....@.....@.....`...L.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-file-l2-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.749541592055871
Encrypted:	false
SSDEEP:	192:2WBhWCEWYnO/VWQ4mWA8WgoqnajKs0V9x:2WBhWlU0WnlGs0VX
MD5:	47B4DF281BE629B8823AE65946C51479
SHA1:	B2D0E2762FFBF1668AD059DDC3BC3404D9130465
SHA-256:	B2BFA9DE580940824B81A96067D5715A14638F93F18EBDC9182A1DEEC3443CE8
SHA-512:	91CAE8D061B99545489F5F99613FA297223EBB1C478E791F5B276DFB18101CE4F24982B5A6A01956DB19BC6B1C93E19FC862D55BE3F6245944C54347E9E0D744
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...+v(.....!..... .....@.....QE....@.....`.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-handle-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.653663560483679
Encrypted:	false
SSDEEP:	192:T/WBhWQWYnO/VWQ4mWHNcoSLrMhEqnajKsZ9ozfO:DWBhW+URBjlGsZIm
MD5:	3C8648161E4FBF415E888626EB927957
SHA1:	485BDA61BCEB014B3E7818E98C4642A87CF1BAE3
SHA-256:	E02506F98B4561BB3F6C07C6D9927649AD2FA7BFCB3174A5BEA29861739B6C55
SHA-512:	2A05FF6B12D9E9B0FBB5FE831A42917C930CCA2AA268BC1D7A27E05D2022F9584AD6D5D52A78DC805AA2198BE85F3442A2AE6B74F5AFE1C55493A43924C8A8F1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....D.....@.....`..._.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-heap-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.597715516660009
Encrypted:	false
SSDEEP:	192:eMl2WBhWEWYnO/VWQ4mWFgRgoqnajKs0VZw:eMl2WBhWyUFnlGs0VZw
MD5:	5EC595F2EBECD32B35AD2DFB2822EC73
SHA1:	03766443ED42646761B5B194C402B8123C22D876
SHA-256:	D5F66804C31B26E79619601B87D313B55B7F7B94870622BB04F7C0AADA8678AE
SHA-512:	A2B32B8271B3F78C4945342FAAF6A59B528317C67F7360D6D81E1EB09961F690EFE5906639F4AEEAE735327796B6C84D2AC154614A4EA3F019241F047A659D04
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...3..U.....!..... .....@.....p....@.....`.....0.....!.....T..... .....text...h..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-interlocked-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.6473154908472525
Encrypted:	false
SSDEEP:	192:GV/YsFEWBhWnWYnO/VWQ4mWWbUjELrMhEqnajKsZ9D1T:GpYsFEWBhWXUeEjlGsZv
MD5:	0BDC5D21A0F3A13FFA5C88A939C8C94C
SHA1:	54A9BBBAF4062B7DABEE866CDD3AE49DB8BA0255
SHA-256:	B7BAAD7A6A3CF241CC00AFA0D126E68C1B0E42CC563335F74372C323CFEFD4A7
SHA-512:	5DED56185CEC4E912FAE9DE1CEED14F5CFE783F097BF79DD23C0040DAC24B3B1B98A50F8E17065A5014528474DFAF141DCD26DF45F366AB5C2E580CC158F3 1C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....}B....@.....`...Y.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-libraryloader-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	6.608486508464964
Encrypted:	false
SSDEEP:	192:xxvuBL3BBLsWBhWcWYnO/VWQ4mWLqP0h64EHsqnajKse3p0jGl:vvuBL3BGWBhWKU864UslGse36Gl
MD5:	05C848C3D74ABCF7443A05780EA3AB92
SHA1:	102038B6E371D38E4CFED0DB8AB8B6FDACE3F0BE
SHA-256:	96849368DD248502827EF59EAB2E7F070C7A2D245261F4124C2B8AB10870FA4B
SHA-512:	40CDF8BD38DA83D237DC669621DF4BB9B90F09B6789352B10135FB14D41519CE84B9311493EB94D7E57C54CD632EED8599316EC2673048B589C08628F89D03E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....@.....`.....0.....!.....T..... .....text...n..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-localization-l1-2-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14800
Entropy (8bit):	6.540043552122422
Encrypted:	false
SSDEEP:	384:YOMw3zdp3bwjGzue9/0jCRrndbBWBhWPUcqslGs0AkS:YOMwBprwjGzue9/0jCRrndbU0Quj
MD5:	1F41511531BBF040F80DCEBE78155894
SHA1:	22B2DCA8C6F4BC1AC7E6C47E23B895DFC185B9D6
SHA-256:	D4A2127300B6AF2E0DABE99BA7D72E6C852800666BD0E8C157553EBD43BB9BDA
SHA-512:	29D8EDBA45EAD782D6438684257209CEAC79EC270124F9A4084EBE86468D304E9D7F690BE5C398D0A1D937537F78B9B43A77379A1FC6E516DF9627775C9DC10
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....g.....!..... .....@.....@.....`.....0.....!.....T..... .....text...'..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-memory-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.648621018514993
Encrypted:	false
SSDEEP:	192:dYxNWBhWMWYnO/VWQ4mW26Ug4EHsqnajKse3p928:dWNWBhW6UB04UslGse3W8
MD5:	8B0AD9B09637E82720831A1D569068A0
SHA1:	ACAE75F37ACB33DF2A72DCA33DEEC3CA5A0A4914
SHA-256:	F2965D9123AEF9C8BD49200C1F07E8E9E0B829134E5B83AF6EED92CC83B8AE35
SHA-512:	34C0F24289E62209FCB093CA5A13955F2EC7BAAB7D7E94D2D06B3B40571742AFA26E54A915AD598699283423C7313329F0417C70B00F3ABA76A4991E2CA91652
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....!....@.....`..!.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-namedpipe-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.743980690618845
Encrypted:	false
SSDEEP:	192:uWBhW9WYnO/VWQ4mWkb4EHsqnajKse3pkXZPo:uWBhWNUj4UslGse3SXho
MD5:	80B207D4C097E89089DB871218FF1E61
SHA1:	0D8E9F07452520C52D931B6C7C6926C44DF292DA
SHA-256:	90645C3729039D54191FA7E17E520A38B2EE7110AE541385D8F3231DB57D5855
SHA-512:	8DC849B523656368FEEF1BEE2E83A53BB4D7DA5417736490B1DE7E6AA63BC3AF49345941E9D9C93EDF92087C75CF6709E493C3A38D3CA879A5D11B00C4E8AD 1A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...rw.....!..... .....@.....8....@.....`.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-processenvironment-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	6.6256208208513945
Encrypted:	false
SSDEEP:	192:F/WBhW6WYnO/VWQ4mWoyLrMhEqnajKsZ9nc:F/WBhWQUOjlGsZC
MD5:	4CE2581038D217453CDCD11F082F9A52
SHA1:	1F47B61805881C9B3BCE0D954ECA9A6AF34F83BC
SHA-256:	CF49C84BF62726928F5F75C4D08E2BFF74B5DBE710C8E914EA26104BCBED2302
SHA-512:	C999489C6618AD50E2256E9DB6366068B8B613FA518213D9CD48356DBA2C133688C5ED489133364993D5E6361DB1F94A9FA75BA034599F38A45C439584DC3F3E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...\..D.....!..... .....@.....*a....@.....p...G.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-processthreads-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14288
Entropy (8bit):	6.534222066734385
Encrypted:	false
SSDEEP:	192:+/8uk1JzX9cKSIdWBhWuWYnO/VWQ4mWdh3lSgoqnajKs0ViJ:A8uk1JzNcKSIdWBhWUU4EnlGs0ViJ
MD5:	CE3240C6D2768D60B70FFA3D3844B172
SHA1:	DADD22D79FAE4AAFB23BD8131C0DF4899AA5976E
SHA-256:	FAED7625C78B6E040AE62B9D37824286724CF6776A2B9BBD728E21F5FFA97852
SHA-512:	0B8FAF0F51A3C79A906C9A084A49B1B5E30872065BD9D523D91DE20B6A6D65BE136B6CC970E8F547B80C3AD8C5A241697B6D1A92BC31A85EAEC2A85A45C3AE46
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....0.M.....!..... .....@.....^....@.....`.....0.....!.....T..... .....text...C..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-processthreads-l1-1-1.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.678158514324658
Encrypted:	false
SSDEEP:	192:ZkAnDfIe1WBhW0WYnO/VWQ4mW6mzLrMhEqnajKsZ9Eeu:ZkAnDfIe1WBhWiU8zjlGsZvu
MD5:	CD7430FFCF4DCB98DF8D78DDCFF1006D
SHA1:	D68E704166581AE79F8E8EB3CF08DBAA29701D86
SHA-256:	2F9747A23A0A8BD1C6E70B3BC015DC45F8A9A8EEAAD96CA2302BD3E0C33FE63C
SHA-512:	A77F78EF0D75D2DC5B5C1106AED4DE8CFDCAE2559A5AE50B73C098892B7DBE7F99E8AE3A25476A02EAE393BDDF37B376A60845903BFF978DF3C78DD7D5671512
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....+&5.....!..... .....@.....I....@.....`.....0.....!.....T..... .....text...:..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-profile-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.610965869568621
Encrypted:	false
SSDEEP:	192:CyWBhWIWYnO/VWQ4mWZNcXFrLrMhEqnajKsZ9V2M:CyWBhW2Uic1jlGsZbH
MD5:	700D4B768074DB0C0C3BB6DB65F32B22
SHA1:	6B6014BD328D1F0543BEF7BF0EAA811BD4968BB8
SHA-256:	C0AA88C945072BABC04E549B9085EFE483F2EB2F60C66502FA68D956E45334C4
SHA-512:	BE47014E32F505742C011DBA215D5969927E008DF41A9107AEE3EECBD617EB7DBB03F453D0071C4FD2DDEDE0B33A90EC6DC1CFB4135D31DE8ECEA1060DB4632
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...p.....!..... .....@.....i....@.....`.....0.....!.....T..... .....text...5..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-rtlsupport-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11744
Entropy (8bit):	6.606845307408541
Encrypted:	false
SSDEEP:	192:BGhWBhWKQWYnO/VWQ4SWUeJqqnajN6z1Yf3:BGhWBhWK+Unlp6z1w3
MD5:	8CB7321D590EEF0CC48D643D1B9D7C9B
SHA1:	ADD669DDCAF9A23BBF524732C091F71E7E5BFE91
SHA-256:	5BA725F1BC75C40D0A5A0A607F843E5C4E86292DC01CE1BEFB86EF46421DBCAD
SHA-512:	BB74B6B26C4E9DA288B8B2E1E0CF4AF47CF41D452EDB33F0D3BF4D653CB3C199A924B4444122045992EC6EBB87308BAFB0EB138260041A9C2AF464BC7B57D4 6C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....tR....@.....`.....0.....!.....T..... .....text...H..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-string-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.703890024796369
Encrypted:	false
SSDEEP:	192:a4yMv1WBhWOWYnO/VWQ4mWEiggoqnajKs0VV:/yMv1WBhW0UKgnlGs0VV
MD5:	015AE28F41E02E57703882CFC3521765
SHA1:	75FDD3A2AFD413A14B9C47209EE15647EE3F456A
SHA-256:	5739D3AABBB19D8985C07284EC7E7F8E9591FCA8D6BEAB4D16B7FF22CA192CB7
SHA-512:	DBF7B977C5E0C82417756B03D160D055A5E517F3E361ECE88C737DF3C04569BF7B40CF1ECC87365613737A3ECC850FD46FB706CDFBC37D005662B9CCC9C6D 9D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...9.....!..... .....@..... ....@.....`.....0.....!.....T..... .....text...R..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-synch-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13776
Entropy (8bit):	6.598439617023524
Encrypted:	false
SSDEEP:	384:pdAdv3V0dfpkXc0vVa7WBhWTUWqslGs03F:pdAdv3VqpkXc0vVaywG/
MD5:	2D219A18F1FE5C5BCAB889BF74817456
SHA1:	97AC747DB3E7BC3ECB2F359894EE0E9C5E4F09B8
SHA-256:	AE59BA27E040D2A3651581B2CA3948006B2E70DCDD7DF82243679C38D4980D7A
SHA-512:	346D9E101E931C0AF54074C702A29151149B049F2458E3392517D93090DAD1875B1850907516CDDB933044B4C8A66936173F2034788C28A7CD0FEAFEE05EA2C9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....A.....!..... .....@.....J....@.....`...V.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-synch-l1-2-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.723942882700585
Encrypted:	false
SSDEEP:	192:vc5tZ3UWBhW6WYnO/VWQ4mWK3ygoqnajKs0VHb1/a9:vItZ3UWBhWQU5ynlGs0VHb1/l
MD5:	880908BF98C7D3A67998470B3770AF19
SHA1:	E02759642BC39F588C51AEDFE1058F727B95EA53
SHA-256:	82B50A82E16B54233B95EC63A8EC99D86844ED115796F60C4B00494C1E15BA26
SHA-512:	7C4047D0F1708312AA9E9CB3F2466746E1F571E4A93AC90C6BCA58004951B64E974A6248756ABC4A55AFFB99511C6FF9DA087F9EF8E2B921FC6AF9BB581BAC4D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....o....@.....`...v.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-sysinfo-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	6.621070064200597
Encrypted:	false
SSDEEP:	192:8oWKIMFIWBhWhWYnO/VWQ4mW17VgoqnajKs0Vnkmli:8JtWBhWhUmVnlGs0Vnk9
MD5:	B15827E6DA414B0EAF28983A032CDE60
SHA1:	429647AEC3681BA91FE2944490C212C05CEF5F51
SHA-256:	AD14B0E3EB3CE3CFDBA79A68A8064EDB62A11FBE354833345C4AE6126E743907
SHA-512:	418813A8C845777E2116871ED1C9039B69BB34938D9E9E85752539E9DF6CCE9B3B21463CDA77D8BCB2AE88625410B2B4D20E1D7EE40624CBA7F0DC057D01D2B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....e7<.....!..... .....@.....W.....@.....`...E.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-timezone-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.711717221941304
Encrypted:	false
SSDEEP:	192:wyqLWBhWeWYnO/VWQ4mWjxQeyW4EHsqnajKse3pAQ:wyqLWBhWEUDW4UslGse3D
MD5:	4C55353E8F13BBF2DEA1F11CE7D34B79
SHA1:	6EA85FDA4231ED7DC537D0C0DFB36F25CB00A190
SHA-256:	3EF9C1B03931B54E98D6426822A634378A64754CB8FB509DF20B8C8072DD8F83
SHA-512:	ED0EF686668A80207AE644F8396D873457FF23D5D6E24B6E1FF87B4BE632A65224AF987A411B9FB3F9FDB197C456B71C6590AC8C2FDC823787F76798D1A7ADDE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...u.....!..... .....@.....@.....`...E.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-core-util-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11728
Entropy (8bit):	6.640499789236732
Encrypted:	false
SSDEEP:	192:zWBhWiWYnO/VWQ4mWQR4LrMhEqnajKsZ9AIw:zWBhWYUajlGsZN
MD5:	4E8F314A1FC6A6EF9CAC0B9A0C4A67FC
SHA1:	700A6771D874A96B0B4C287ECE399C98A012B6F1
SHA-256:	BBAA4FD9157D92DBE443CB6C9BD51D2E88D1497DC852ADD6B5D06E462FC599C5
SHA-512:	53DFFD2354D438420587E1C53267739343E04A7D8D6A29F02867F3571A5064DF04B9B082D8835D9C174BAC85D01B7B3A699542BE41C70503BB7641028287DD8C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....v.....!..... .....@.....(I....@.....`...9.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-conio-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	6.646138241902779
Encrypted:	false
SSDEEP:	192:FnYm2WBhWCWYnO/VWQ4mWt4goqnajKs0VII:6WBhW4UznlGs0VY
MD5:	5BABFCDBE7E6A051CBB46E92D2B1D374
SHA1:	9DFEC59A4DAC8F2B428B0E5F680983182C75F9EC
SHA-256:	A57A01F9466F3152B17F03A1E66D7D394AEB0EDBE8F9CD8CC49B4334994B831D
SHA-512:	F1EF6E61C6639FD116F4D512AAEEE4F3F0A8B33453B0AE33B735949FE7BE047B3DDD8EB1483A328E5936D977A137E510815E7EFB376767C7505F3D2AA3AE072 9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...U..r.....!..... .....@.....@.....`.....0.....!.....T..... .....text...P..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-convert-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15840
Entropy (8bit):	6.454026885121232
Encrypted:	false
SSDEEP:	192:rT7cyZWBhWDWYnO/VWQ4SWS3+RJMvN/qnajxg8fS:rTgyZWBhWDUU6/INvq
MD5:	E28F70E327F9B4926D6484DC1A159C94
SHA1:	FDA05D5E0562083801966B3F962D265A6A8855E2
SHA-256:	DABCCCC0F209E83D80024CD063D4E16D2CA2478B483E33DB7CFF40976C3C993C
SHA-512:	89B3B1F65137BF2400C784B934FCD0349BA00675902B2FE48971246E6E1C99423A3B5ADADA797753A7A6F35F50AD980A8404D5A18CFC3606B5CC52B278FB13A(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!.....0.....P.....@.....p.....@.....!.....T..... .....text...^..... ..`.data...@....0.....@....rsrc.....@.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-environment-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.618891411839505
Encrypted:	false
SSDEEP:	192:1odpWBhWlWYnO/VWQ4mWRoh14EHsqnajKse3pV/R:16pWBhWVUxh14UslGse31
MD5:	06B191B4F4A1F1FB86BD826AC5F48C2C
SHA1:	B7B454CA07B984FB74C756E60BC4EAE0BC6991A6
SHA-256:	6666E2FAE294C82EAE55B33B6C4A61463DCA84C4B411E03326A71FDE333B519D
SHA-512:	638856717A5DB0E5BACEBA54CF596718C661420C4985DD279A78D42095CADD64527DD2214F0D4E35DE7AB4D531444FEE2CAF5F5941D32C28878FEE2C3B67CE F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....\.....!..... .....@.....@.....p..".....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-filesystem-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14288
Entropy (8bit):	6.515762527300964
Encrypted:	false
SSDEEP:	192:bnWlC0i5ChWBhWnnWYnO/VWQ4mW68BAUOgoqnajKs0V3:bnWm5ChWBhWnXUDpnlGs0V3
MD5:	499F30D39C72E8620A30BC4E0C7985EC
SHA1:	D57FE510B27C16FBC11BB2042333894ACB5914E2
SHA-256:	A4EE1A6246A4C0612F12901298323612AD4C738429D14075942329CB5AC807DD
SHA-512:	8DB7E3B17474A1462A99E19BB35690B966424EEDD632455AC00DAFA9CC46569BD6E081C36DA52B9C78237A85493C7ABF217D6C3A69098C73BD8C18633B4A76(C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....f.....!..... .....@.....-....@.....p.....0.....!.....T..... .....text... ....`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-heap-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	6.59337335302922
Encrypted:	false
SSDEEP:	192:reY17aFBR8WBhWjWYnO/VWQ4mW3pUnLrMhEqnajKsZ9bx:rzZWBhWjUKUnjlGsZT
MD5:	A77F681BE0EFA335EAFC0C5175CCEDAD
SHA1:	511D3078D142C672FEBF012BED412660F88299A3
SHA-256:	434C2CE6CF4E61BB4273C7EFB39565445383CF77A8BEE79C41FFEB5315B6F285
SHA-512:	12C440B9AC908E934BC419A520E2BC8697E42CCC438B46AAC34CE98AEFE816FA18D1F3073C01D59B65FE21AFC65435B27B6D3398BF5361B68DC30630FA4C6C 07
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....-).....!..... .....@.....d....@.....`.....0.....!.....T..... .....text...v..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-locale-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.717763097244974
Encrypted:	false
SSDEEP:	192:YxZJ2WBhWQWYnO/VWQ4mWZG71LrMhEqnajKsZ9Ron:YxZMWBhW+UNjlGsZe
MD5:	0B688C4FCE6D07018D443C1B3BFFB3D0
SHA1:	0F2CF0F20FE7CFAF7F8F27E7AD7D5E1871316756
SHA-256:	FB22B002939BB699BFA1F25B3B4C96E71CB5A737183ABC79A03A22C6D517A1A5
SHA-512:	1F555158A1D98624EF32293B3078F4CC20B1107157E2B48E36D3248371519610852 75FDD581081FE1E0D62EDCF02197C57FDAE972EA20378BD3E4F84B99BFD3B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....!..... .....@.....@.....p...e.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-math-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.202005954734633
Encrypted:	false
SSDEEP:	384:fQF2KmbM4Oe5grykfIgTmLuWBhW3UnjlGsZN:ftMq5grxfInR09l
MD5:	547E74027B6DB8C65BBEE2707335CDC4
SHA1:	C7CE2446BF4DC38D72EF115BA67086C4F121C7E8
SHA-256:	35E617878BF8B927DF3387C5BDAA4BA94309C7AFB0F901C6A53326C3CC97FB15
SHA-512:	6BD92F9C3DD20B75FC18DE1A88C82FAC4D49B81B652A7DAE109AB64DF5F109E9BBF9842C2BED2148D24368B2F9BE82FB86A824032C073CE37C61C657EDE74BD9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...h>.....!.....@.....`.....@.....`....+.....P.....6...!.....T..... .....text...7-..... ..`.data...@....@.....@....rsrc.....P.....2.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-multibyte-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.204292997926146
Encrypted:	false
SSDEEP:	384:/7aLPmIHJI6/CpG3t2G3t4odXLtWBhW+Upz4UslGse3PG:jwPmIHJI6OhUS
MD5:	5A82F00442E6C0558687E4C8FFE8D00C
SHA1:	98794532EDD7627D8D4EDDD064D314C2681F8E78
SHA-256:	559286B7F6B575E7AD881824364D5F1790669917C55EB6AA073DB0B9068AEF78
SHA-512:	6CEDAE2F524AE6CFD16896653957431E8D4647050EC405977CD957E8B8E2CB120E525CC16BAF7382DF7E5048DBB574EE509481E7F11477462B5AB0AFAC89349F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...r"A.....!....$.....@.....`.....#....@.....p.... .....P.....,..!.....T..... .....text...d".....$..... ..`.data...@....@.....@....rsrc.....P.....(.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-private-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	66512
Entropy (8bit):	5.530731860428242
Encrypted:	false
SSDEEP:	1536:V8tbDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPgynT:qtDe5c4bFE2Jy2cvxXWpD9d3334BkZnA
MD5:	A407FC4E6705A7FFA7CDD8264266FBE4
SHA1:	7DAD59D1A1A626A483E1EAFB839E9859CA99C6F5
SHA-256:	BE86CF37B09C08EC4EB3CF7E8403C7BB86EE80441323906D0DDACC884F3C79E4
SHA-512:	E8BE910F4BDAF997838F783668457A207D990E40D62C145E7387049B1F81D21299A10B91E141307630A792D0CA226F8235D311263DBBA8493829B82E547F6932
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L....m.....!.....\....@.....p.....!.....T..... .....text..... ..`.data...@.....@....rsrc.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-process-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	6.618753441548937
Encrypted:	false
SSDEEP:	192:4kW9wF5uSqjd75WBhWUWYnO/VWQ4mWGxVyILrMhEqnajKsZ9h16boE:4rcuSYWBhWCU5jlGsZPcP
MD5:	80A4CBB957D7222EE43917B149E93C53
SHA1:	01603F8F1642D624BBA3BD45C5D73D9D10001BE4
SHA-256:	C24FDFD9BA4701BFFB2AD840FFE315CD807BEEA6748B97835E0675C35DD13F47
SHA-512:	9C981D3EF9FC22D4C459A0139621D6DACC43A6C343462FE71A0BF885C3258184A6C4F4AB11B8E1429C11319FC0401BA6EB64E50B4629DA94D177165BC44639E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...*4.....!..... .....@.....@.....p...x.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-runtime-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16848
Entropy (8bit):	6.37698990107166
Encrypted:	false
SSDEEP:	192:O9DMjOOfhrpIhhf4AN5/jifWBhWGWYnO/VWQ4mWHQx4EHsqnajKse3pJV:O9ojOShrKkWBhWsUL4UslGse3Z
MD5:	898F86B6B29142428E92956F9043FCB5
SHA1:	89970BCA1287CD9A28AF90B1C7E61CFAD6F8D716
SHA-256:	7D6F4E5C3AC9DC87FC962F515A0173D75718DA6B6FFCFF4F9255C109E7FE7A18
SHA-512:	A5444063C70A790EE9A339EF45644704CE75824D007F90CFA570C7C3E8DEB0DD7852A9F7B97CF0AA82AAE05D6FC0CDAF618DF9BB7BDADF39B6DC609A40F2C 363
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...z).....!.....0.....P.....@.....p.....@..... ..!.....T..... .....text...5..... ..`.data...@....0.....@....rsrc.....@.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-stdio-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17872
Entropy (8bit):	6.410004360781716
Encrypted:	false
SSDEEP:	192:/y4x+m9uWYFxEpahfWBhWzWYnO/VWQ4mWLw+LvtugoqnajKs0VvY:xx+tFVhfWBhWzUuv0nlGs0VA
MD5:	4D46C692A087DAD81BEEC8211F67F4A3
SHA1:	DEA942FF2135EE50FC45861D7D6F9CBD8817316B
SHA-256:	DD4A1885415CF5C37471B18FBD9211E0B4887D0456A3320D0213FDDC4209E66D
SHA-512:	D48FECDC6179C193349934F3D14A1C5196F832364F89EDEADC55329CA6E4899D49659B87EF6C06ED741012F96F10FD5C8B04497411E95880728FDCB79DC6155
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L..*.....!.....0.....P.....@.....`...a.....@.....$...!.....T..... .....text..... ..`.data...@....0.....@....rsrc.....@..... .....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-string-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18392
Entropy (8bit):	6.292455454608518
Encrypted:	false
SSDEEP:	384:7KgSx0C5yguNvZ5VQgx3SbwA7yMVIkFGl7WBhWSUesln8ppy:Gx5yguNvZ5VQgx3SbwA71lkF19dvy
MD5:	C3F7F531A0F4A3BC4DEF8191803336D3
SHA1:	68DCC28EE07004823C1ADDD65C478ADA06A8708E
SHA-256:	DCF381E5995FA69E3902A3F49464EC5A35F9E78A55444B24F49717512FD37372
SHA-512:	7784AAD3546620D9EB802C65D50DFAB4AA32F15D32B8D71F16D92E5446394F9B521527668E547C3EFDDB959DDEDEB623A880975CB0751FE1B58BEF94689B71F D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....b.....!.....0.....P.....@.....@.....p.....@.....&...!.....T..... .....text...O..... ..`.data...@....0.....@....rsrc.....@.....".....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-time-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14304
Entropy (8bit):	6.557683602083814
Encrypted:	false
SSDEEP:	192:lugzjVDuWBhWlyWYnO/VWQ4eWuya4jqqnajN6z1zX:luA8WBhWloU00lp6z1z
MD5:	AE8E8A8CCDDD31C6E93C23D66CC2C7CE
SHA1:	E49D67BF5B5E5A1B5F2564603AF59523305AD3C1
SHA-256:	66E10B3EAFB86BD0B31C3AA494DE64F01B9908B90022D1C6577FD639C337CDD0
SHA-512:	F85D2ADD7EAEFB2D49D0E776720DB659587DC884D943339DE8F95354C965F86D36D06A3DE81EF5673EB18BF0E84F660B76EB19BF4EEA73BDD51A497C2ABA8 E6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L.....D.....!..... .....@.....VK...@.....`.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\api-ms-win-crt-utility-l1-1-0.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12240
Entropy (8bit):	6.694309765478122
Encrypted:	false
SSDEEP:	192:cCnfHQduLWBhWpWYnO/VWQ4WW6SbgoqnajKs0V6f3:cgfFWBhWpUAbnlGs0VI
MD5:	23555460EB85D497549C959179118690
SHA1:	704E67C82FCD099E36958429EA65C24DBB4728AA
SHA-256:	C4073E7FEFDBD189C61F63A6C8AFD169F35E2272B035ED49B6517419CC7114D9
SHA-512:	8151BBDF18A420B5B5E7CBD4F3C3D66100469088986FC4FFA893F1DE2E850FEF1FD1E2F674057130336C3FB4E0215008CF6FFEE4164BC1DC5E87BEF6B79E73C 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~v..~v..~v.5.~..~v.5.v..~v.5.r..~v.5....~v.5.t..~v.Rich.~v..... .....PE..L...f.>L.....!..... .....@.....@.....p...^.....0.....!.....T..... .....text..... ..`.data...@.... .....@....rsrc.....0.....@..@..... ....

C:\Program Files (x86)\PWMinder\runtime\bin\awt.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1303040
Entropy (8bit):	6.574171008377848
Encrypted:	false
SSDEEP:	24576:syHfb94EA+3D+crQcmZD3a8MszHfeU4f0eM8wrq5i4ikXB0Xi8Md4oy2J1:/eycNciXiNryE
MD5:	9E24051A4F890EA6CB7ECA4F03873E92
SHA1:	99CD15E873E5FD4687887A998E5BE8186FDCAF39
SHA-256:	25701FECC45301E864D0D033A509951E5D1346D53A313495C201222C32B08D4F
SHA-512:	E8B694BF40C765350190573B3BC49693C7DD569EF5AC601C797FA770D857236C88835E0A7E6C1BAF056F44ADF0B17E1A44E0D99AA7079E75C63DB1FAFA84A5C B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....t..'..'..'...'..'..&...'..&..'..&..'}.&...'..&..'!.&..'!.&..'..'...'}.&...'}.&..'} .g'..'}.&..'Rich..'.....PE..L...v.....!....`.....p.....0.....@.....Pr..0....(..|.....9.....0.....\..p.....@].... [..@.....p..(....L..`.....text....^.....`..... ..`.rdata.....p.....d.....@..@.data.....@...|...2.....@....rsrc....9.....:.....@..@.reloc.....0..... .....@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\client\jvm.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5315584
Entropy (8bit):	6.77885202565967
Encrypted:	false
SSDEEP:	98304:GLoBnyOU01jEhuKqvcVa+21e3XRP2/uQ7/h2OrGLDNeNKonpw3WqgyntfGtptEuR:GLoByoEkKqvcVanc3XRP2/uQ7/h2OrGw
MD5:	4561A29E18F3A0D185CE3179C8B59811
SHA1:	410B2874E370B5848A7E74B3FF5F16C68B348BB8
SHA-256:	2CC85ECD791D0BB0E9F995322E4BC4C27ADFDEC2F6B555B9F228F429A3D6F281
SHA-512:	0D8AC1E7EA1685338E3587301A0B82A2BD70408025F0334A2423310C0430E8D41903048B6AB561B71D20B4CABDDBB03D928EED9BF9B81D720CBA3A4B3246871 6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>...m...m...m..Km..m...l...m..%m...m...l..m...l...m...l...m...l...m... m..mA..l...mA..l...mA.'m...m..Om...mA..l...mRich...m.....PE..L...:.....!.....=..:.....R2=.....@=.....S.....@.....l..6...GJ.h. ...pO.@.....O.8...@.E.p.....E.....E.@.....@=.@.....text....=.....=..... ..`.rdata.....@=.. ...2=.....@..@.data...P....`J. .....RJ.....@....rsrc...@....pO.....M.....@..@.reloc..8.....O.....M.....@..B.....

C:\Program Files (x86)\PWMinder\runtime\bin\dna.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	2701824
Entropy (8bit):	6.397087659167403
Encrypted:	false
SSDEEP:	49152:HW7Qusws1Lm87loZJ05vNJcFHEVJx7iSatdWUz1zq4NarrDvVwaTRpEgUdM:HW7m/7loclcvNtrtZaXrVrzEO
MD5:	43A4F194D1BD475DF8BE444A3A541A9E
SHA1:	6AA5591C56186B378654D717890E7A7EF57E2E06
SHA-256:	19B75CAFB9A376EA352CB7DB5BCBD7B83D8CC32CFED067D41EFC0167FF0EBB8D
SHA-512:	534AD7C5785910209C63DDE4B48AA6BDD7CA1ACFD6731E7CF166FAEC810846C5CA81844311C086DB352BD0A839B50707F2C5DA6B84AABAE59423DD5E36D29 91
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#.....'..do...,.....)..... .....&.x.....&.....&.`.....'..*.....$.&.H.....text..... ..`.data....'.....(.....@....rdata..(..... .....@..@.bss....do....&.....CRT.....p&.....%.....@....idata.....&..0....%.....@....edata..x.....&.....&.....@..@.rsrc...`.....&.....&..... @....reloc...*....'.,....'.....@..B.....

C:\Program Files (x86)\PWMinder\runtime\bin\fontmanager.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	707072
Entropy (8bit):	6.680629415868332
Encrypted:	false
SSDEEP:	12288:L/05aO7jk9/OgHnjCAlwD4X7/TkcrFWhW0/X6:Q5aCmOAlwD4XzTkoqW0/X6
MD5:	FFFC4D904B2EE6EF06084126EFC54723
SHA1:	3F9E9E5E1B2164AA7D4B80EB52A2FC0E7742D612
SHA-256:	BEA9A43B793EE5E9EC1FE3A4A8FB66C70EA27EAF1D340D8CEC65894563CAE45B
SHA-512:	C7CFD183DEA2A77FE85C264743D362ACBF3045A3100A000CB0BF4595A6B87855752D221E51D4C3DE254FA256018262C49617070F7F66F984BD1B1D1BE1B21A5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u..1..1..1..8.K.?..c..3..W.%.3..c..?..c..;..c..6.....9.....6..1.....9.... .0....'.0.....0..Rich1.....PE..L...Uo.S.....!..... ....@.....}..X...X...@.....|C..@q..p..... .q..@..... .....text..... ..`.rdata...s... ...t.....@..@.data.....z.....@....rsrc.....@..@.reloc..|C.....D.... .....@..B.....

C:\Program Files (x86)\PWMinder\runtime\bin\freetype.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	444416
Entropy (8bit):	6.7233291629141805
Encrypted:	false
SSDEEP:	12288:uy+KmKfK2G6pZsoLrYRnSftcE9AHRfEWm:uy95stRS1zA6Z
MD5:	4A2588F93EFC2DD881FCDA0FDEBC3DA2
SHA1:	BBFE68DB7AA602FCB2EE40B97188509C55C438BF
SHA-256:	DEB6FBF34937D6E0AC1ED440394432DCC54414D41BFF541BF461E248C93C037B
SHA-512:	10FC0614B9C232688756F66D6D95AE9090BFB4163E10C9B5F6E2714978F60141EF3903A238715BE545748686249CF87367C423C8EDFA93F6DF884112810BF512
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T..w:..w:..w:.....w:...;..w:.v.;..w:..w;..w:...?..w:...>..w:...9..w:. *.>..w:.*.:..w:.*....w:.*.8..w:.Rich.w:.....PE..L.....}f.....!.....|.....0.....@.....p.... .....@.....0.....text...<..... ..`.rdata..Z....0.....@..@.data.....@....rsrc.....@.. @.reloc.....@..B.....

C:\Program Files (x86)\PWMinder\runtime\bin\j2gss.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	33792
Entropy (8bit):	6.153540960210045
Encrypted:	false
SSDEEP:	768:SeJRbKoEKPizoqi/qDXTbCa3qkwi2u1yjklsd6TeLt:eFP73Ca3qkwi2uojklsd6TeL
MD5:	688B661C699D297FA91BF1CC9496925D
SHA1:	9736E9A110CC9B2EFF91BF61F714781F519659ED
SHA-256:	E906AC8AEEAE701DC610DDB8DD8211C713FE578802E290D0D23744AE23F53EC5
SHA-512:	1442B3C65F047ADEE713BE3B8012DD37E25A019D641237AA6520A95FEACDDE7A5FD9D74E14AA5B75C384BA8EBDF1FB98692A853E563EEFFC71FCB2EC4A88F 404
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.....~.....m.....1.....1.....1.....1 .....Rich.....PE..L...(.i3.....!.....B...B.....G.....`.....@..... .. ...@...x.....X}..p.....}..@.... .....`.....text....A.....B..... ..`.rdata.....`...0...F.....@..@.data.....v.....@....rsrc.....x.....@..@.reloc.....|..... .....@..B.....

C:\Program Files (x86)\PWMinder\runtime\bin\java.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116224
Entropy (8bit):	6.676393258155189
Encrypted:	false
SSDEEP:	3072:paqXlHyktTPKrh9kUQsxIftGTAnbNrcGbQa:pZFykEhGIB
MD5:	ADE0F55D07E461AFF38C5FB4829B2621
SHA1:	66E55A36A1DA7867135FBDED13F2A047F061440D
SHA-256:	F2A78836F090A8799A0EAC139E65933AEAAC2EAB6ACC63F9F603B0EC7B279B00
SHA-512:	143CF638EF0226AC38AFF582C37F09A65E88F21DB5AE8CBB9373216D2344AD251D3645618E3AE465F8CA01761D6D555C9C5724E49CC75D9BFB5247BE645FB3A C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=[..\5..\5..\5..$...\5.)4..\5.)1..\5.)6..\5.?,4..\5.)0..\5.?,3..\5.c)4. .\5..\4.]5.c)1.\5.c)5..\5.c)...\5.c)7..\5.Rich.\5.....PE..L....._.....!.....0.....@.....R..hA..... .lM..p.....L..@.....0.. ....Q..@.....text..... ..`.rdata.....0.....@..@.data.....@....rsrc..... .....@..@.reloc.....@..B.....

C:\Program Files (x86)\PWMinder\runtime\bin\java.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	6.199341275883711
Encrypted:	false
SSDEEP:	768:0/WrG/tM8vM5R2TyJ5R3s8D/bkt5Ruz3Vb3pRs5T:0/WS/dM5RdJ5R3sozkt5RA3pRs5
MD5:	61614DAE01803AC917287B511101C3DB
SHA1:	94296ACCF74389FA1CF94108A9E402AE268F8B84
SHA-256:	0EB74B638CD964C0B29E6F67B9AA266B0FA9A48352D08419BC1D728369948BA9
SHA-512:	073EF0D5EBD1900FA3C889FD3CC610715C946D295CBD23A20B1501F41681396F590835663F8A1A477CDC2C43C5D5A160821912A113116602B796FF52FCAB2F99
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....Y.....Y.....Y.....Y .....Y.....Rich.....PE..L...Yr.....~..... ....@.....C....@.....P&..@....&.....@..Hn.....!..p..... ....."..@..... .....text..... ..`.rdata..0.... .....@..@.data.....0..... .....@....rsrc...Hn...@...p..."..... @..@.reloc..... .....@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\javajpeg.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	140800
Entropy (8bit):	6.4367807686163525
Encrypted:	false
SSDEEP:	3072:nDk3B+ABFXE4aDOGHbfeGnmNMtDUUUASi14vk2pE5:Dk3B+SFXE4aDOGHLL/cFvkd
MD5:	6AF183D27F44CB749BF55D474F02B33E
SHA1:	E253EC96F965CCFC853A4BFBADDF430EC06BA3A2
SHA-256:	A3CF0A3171B2036292CF23DD923E8576CDA893251D5FD899C5F742FCBFB62509
SHA-512:	89861213AB2F72136B5A6A41C9E2814D22C4BD453708CD8FF118107696C1D9C9C8E379AE3B9833A7F641882903A3A1867AC327967AA5DEB314AE7884616FFFC7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F.....P.....P.....P.....P.....,.....,.....}.. .....Rich.....PE..L.....i.....!.....H.....W.....`.....@..... .....@.....P..0.....p.....@. .....text...)..... ..`.rdata...4.....6.....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..0....P..... .....@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\javaw.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	6.202871651600686
Encrypted:	false
SSDEEP:	768:VAziajzM5R2TyJ5R3s8D/bkt5Ruz3Vb3U+r5:azLM5RdJ5R3sozkt5RA3U+r5
MD5:	777CAC3523828605EE329E372AFA9570
SHA1:	C1EFEF51F323E3BA27E35B6979F1EB74F98D9157
SHA-256:	0F88DA0A2E3AA557ED24C758C72EF69FCE2898CB8EFF8D2CC2FA16036EC61ED4
SHA-512:	1DF4D7AC8EAD2A150229FA8CE6F50F567C68416639E97CE57AB25C92685B91E771832A3A4D624A0035BB46FC69EFD89F6DDFD0C7C66D3645F8057E860D1ED24
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.....I.....I.....I. ....I.....Rich.....PE..L..... ....@.....@.....<&.....@..Hn.....!..p..... "..@..... . .....text..... ..`.rdata..... .....@..@.data.....0..... .....@....rsrc...Hn...@...p..."..... @..@.reloc.....@..B. ....

C:\Program Files (x86)\PWMinder\runtime\bin\jawt.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	5.156022742858668
Encrypted:	false
SSDEEP:	192:Uyx7G4o41NyvUdZtzQi9L98LjOTpmzPRts6lu8RIN:UysKNBdnQo8j37RyURl
MD5:	37829FA6C09A1DE70475F2D562CE276C
SHA1:	66022C315F9B38519693C5B97A00D154C069B294
SHA-256:	7194E616CA841B0628B9E7F45F3B0C470D25B0D4C5CD41D0485DFBA504261AC1
SHA-512:	DE352D83447D2716E1C75E9DB9834059144BAB3C86FC7CED9F8F360D5EF5D68C2AF2AC06586A3789205468CB33E3FAD5A3FB0BD84527A73D9C71A7FFDBDE8I45
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M...M...M...D.Y.O.....O.....F.....G.....L.....N.....O...M...j..... L.....L.....5.L.....L...RichM.....PE..L.....&.....!..... .....`.....@.....`%..L....%..d....@.....P..`.... ..p..... .....0!..@..... .....text..... ..`.rdata..... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..`. ...P.....".....@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\jimage.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18432
Entropy (8bit):	5.823283435150848
Encrypted:	false
SSDEEP:	192:RWfQMW5PpwtopsVrzfPhiGbDc2qlIupq5l2MAqcjO1oHr8d26G9eYEljs9HfrN8P:MvAu2uZzfpiGbFT5leqcjhL999HfrN8
MD5:	3B76754411B148CDD972BA0CA060F9BC
SHA1:	0FF74CDABD78907C3922E4181A9B58D943765ED0
SHA-256:	F64FE42E360A4746E0A2A28CBF48AACFFCAF4A739B16503314FB663763E30575
SHA-512:	EBEEA757F818A697F2FEB3E34317A779ECB43BCEE92E86F2EB3D7BC25D00C16F670CC146AEE2D89B52DB6D97A1EF1AF89A1BF74564508F0206F4F9DDEE37A 4BB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K.....W.....0.....9.....l.....l.... ...l.;....l.....Rich.....PE..L.....].....!....&...".....*.....@.....@.....K..$...4L.....p.....P....B..p..... .....C..@.....@.....text....$.....&..... ..`.rdata.....@.....*.....@..@.data.....`.....>.....@....rsrc.....p.....@.....@..@. reloc..P.....D.....@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\jli.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	68608
Entropy (8bit):	6.823089556404005
Encrypted:	false
SSDEEP:	1536:5zP6VBc5yzrThwnQVumpIODPnTolfkzIUhwWRRQm:5zP+BmyzBwnQVumDDfTBfathw4Qm
MD5:	7E2A6F8DF5E8282020B9528D4FD11607
SHA1:	58C520450DEA71FBDDCBDD8AA601BD82444AB257
SHA-256:	8F228CB7005DBB91F3214518F735A34A7CA0FE9797BAF47E9EE52B6274A55FCB
SHA-512:	225D59E45CE6F2A74DD3BFE9652C7D1D41FA0821C4F3354BE8927B70545EABD965F8AF7533230B2A8A6CA613A6157FCDCE51D4275918D229853798554B9A321
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..0..0..0..n0..0...1..0...0..0...1..0...1..0...1..03..1..0..0...0o..1 ..0o..1..0o..0..0o..1..0Rich..0.....PE..L...GO.....!.....n.....@.....@.....t...T..... .....0..0...4...p..... .....@.....text..... ..`.rdata..`Y.....Z.....@..@.data.....@....rsrc..... .....@..@.reloc..0....0 .....@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\jrunscript.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.564478703467656
Encrypted:	false
SSDEEP:	192:IujeUrZfvE3Cq9TjOlmTaP70lls82J5pz6ERxa5ARK:pjeEfsyq9TjGmK982HRo5AR
MD5:	30B93A22915353ADF3E985735A2324F9
SHA1:	9D7FC5D2E09995AADCF1EAABDE98AFD78A52F40B
SHA-256:	2BA582F71263B9357D02B09D4B24040448BB43964308BD45893E5E10AFF4A5DD
SHA-512:	5D167480DCB9BA4D53E33E752502D362561C991C27C7901503C1F323A4B1F228E132DDFE74EFE3D3ED6E58F859D8E331B743AD9C1EE0F650FE584A63C8B8964
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........................s..Y...............Y.......Y.......Y ....Y.......Rich...................PE..L.....c....................................... ....@.........................`...........@..........................&..H....&.......@.......................P.......!..p...........................p" ..@............ ...............................text............................... ..`.rdata..x.... ....@..@.data........0....... ....@....rsrc........@......."..............@..@.reloc.......P.......,.. ....@..B... ....

C:\Program Files (x86)\PWMinder\runtime\bin\jsound.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	6.4391165971672475
Encrypted:	false
SSDEEP:	768:0OvuheALy7FZwYV8qwFW4ahh1fT4JQc3tOF4r2c4vZOJAA:0OsLy7FZwYV8qwuh1b4JoF4n4vZOJA
MD5:	AB00C17B04E12E9C35F7891A5297ABD4
SHA1:	ABF9CB1412115AC156A1857A6F588A44C79BF5FA
SHA-256:	4959A9F8111CD761C91A15FF867B39B6AA5623E6F26E4B1BFB07FBD96A402435
SHA-512:	C324F2B3DD45F491565F24E13F038FB439D5153EA743A2B290EF0E512EFFA85C24D1368D17F5C23AAF2BD1D0774705A5FDFA91B822BBADBB6786C2B2800E303 7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$......................O...............................g............;......;......;......;.#....;... ...Rich............................PE..L...p.=............!.....h...@.......n..@...|...p..............................@.......... ....text....g.......h.................. ..`.rdata..4&.......(...l.............@..@.data..............................@....rsrc..............................@..@.reloc.............................@ ..B.. ....

C:\Program Files (x86)\PWMinder\runtime\bin\keytool.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.5467659869352826
Encrypted:	false
SSDEEP:	192:2pewRb5f3E3qD/n/JGI2jOKcc1PjGlls82J5pz6gKOa5A+qK:2pewff06D//JG9jhcir82bKj5Az
MD5:	1E6AA2909616631AAAC5C8D37C96FB70
SHA1:	A47E288A5035666CE3C6DD32E3DB41089647E202
SHA-256:	1EB0DE3ED0CCF1AFE1D696C2CA58642A7049B660A9B9822161F18FD6C3FE7CE5
SHA-512:	30778D54855D79A02DE010DB1C93B45E647744B4BD851F098C9B11895FFEA5D6EE690617FDD471C7846037796D89E7E8AAC6D95D64CA236739BDAF9BA074CB B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........................s..Y...............Y.......Y.......Y ....Y.......Rich...................PE..L....Z.B.................................... ....@..........................`......M.....@..........................&..D....&.......@.......................P.......!..p...........................H "..@............ ...............................text............................... ..`.rdata..t.... ....@..@.data........0....... ....@....rsrc........@......."..............@..@.reloc.......P.......,. ....@..B.. ....

C:\Program Files (x86)\PWMinder\runtime\bin\kinit.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.5557421672725456
Encrypted:	false
SSDEEP:	192:55ewRb5f3E3qD/n/JGIrajOYDMNPjdjlls82J5pz6wPEQa5AAK:55ewff06D//JGEajjIpJ482DPEZ5AA
MD5:	23015C30E3223AE30DF9D6B9C03C5F39
SHA1:	E66C83E06B514750C78E5D7DD1146737806A4483
SHA-256:	984EC51776C8205155FD4C147364D636BD61F40D6FF703F3D8E3A931F81E30A6
SHA-512:	B9F2B22BD491D920A29E04F509CC0EA7B915642FA2D3A2F5B0A9C4048288057039C0BDCAF1B31C15ED37588EA023CA2B53F149617B750331F0D3B1A98D99AF1 F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....Y.....Y.....Y.....Y .....Y.....Rich.....PE..L..... ....@.....`.....@.....&..D....&.....@.....P.....!..p.....X "..@..... .....text..... ..`.rdata..t.... .....@..@.data.....0..... .....@....rsrc.....@.....".....@..@.reloc.....P....., ...@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\klist.exe	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.55385782736454
Encrypted:	false
SSDEEP:	192:z5ewRb5f3E3qD/n/JGIrajOoLPPj1lls82J5pz6IUqa5AAK:z5ewff06D//JGEajTjC82bUn5AA
MD5:	7E5D3DD741C932F221B5AD2221728296
SHA1:	26435F7A82477FABCE837A439BF541F33933AD4E
SHA-256:	30B7A484A2E2CF1BDEA444C1F44561BAD388089155E3ACB093D2FC52EDA19B91
SHA-512:	A4054DB69A4412A878700E26B5F545248D2269C721DA8C81C3B99C70EA07993E7AE3A65050C410FDBC7C0D71EE5FA6C80BCCCFEE24FF5A84A7E3B4603248CF 12
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....Y.....Y.....Y.....Y .....Y.....Rich.....PE..L...C..!..... ....@.....`.....%.....@.....&..D....&.....@.....P.....!..p.....X "..@..... .....text..... ..`.rdata..t.... .....@..@.data.....0..... .....@....rsrc.....@.....".....@..@.reloc.....P....., ...@..B..... .....

C:\Program Files (x86)\PWMinder\runtime\bin\ktab.exe	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.5502642163327875
Encrypted:	false
SSDEEP:	192:75ewRb5f3E3qD/n/JGIrajO8nAlPTfAlls82J5pz66hRa5ACK:75ewff06D//JGEaj7OZ82FhI5AC
MD5:	A84228B4062901C51499E82BEAE51694
SHA1:	EFAEF972104F7F9CFE4E8433986A45DC42E85495
SHA-256:	A3F1579DED60F2A512B0D62C4E08E8105ECA0987419B20FE88A25881E4E086F7
SHA-512:	4E286EF2A9493C146615BFEB2E2059A079583A2E8DE469A314F9DD49445BFC27C0FE9FA60E8E7995E9AA2D2A54875CF675AF636292B1A0BBDD12A096AA5F209 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....Y.....Y.....Y.....Y .....Y.....Rich.....PE..L....7..... ....@.....`.....@.....&..@....&.....@.....P.....!..p.....X "..@..... .....text..... ..`.rdata..p.... .....@..@.data.....0..... .....@....rsrc.....@.....".....@..@.reloc.....P....., ...@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: PWMinder, A uthor: Ewert Technologies, Keywords: Installer, Comments: This installer database contains the logic and data required to install PWMinder., Template: x64;1033, Revision Number: {5EB4ACF9-60F1-4E53-B837-23C8A24DDA3A}, Create Time/Date: Thu Nov 17 23:20:42 2022, Last Saved Time/Date: Thu Nov 17 23:20:42 2022, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Entropy (8bit):	7.996112634596576
TrID:	• Microsoft Windows Installer (77509/1) 63.77% • ClickyMouse macro set (36024/1) 29.64% • Generic OLE2 / Multistream Compound File (8008/1) 6.59%
File name:	PWMinderInstaller-3.3.1.1.msi
File size:	73277440
MD5:	9661ec2a8a20c92f691e50cd91750a1d

SHA1:	092ee11b9c2805f808e0a072c5db1cced5648418
SHA256:	d621d35135fe84d33a85da02b68dd2e327cd01d6185b0cddda98042259c2da0c
SHA512:	93c604fac599af1938458f334be4b47901f48a573762216b496d1fc5fada7740f69c6532d0ba16a96d4e4106e2e9bdb34183f2f8c8e682de0d84d9507134dce8
SSDEEP:	1572864:ofTOkJfGtvX2NxgCl6DSgDRljHMStTHXmkK6Nhb/68E:ofaOGtvCPwZRlDMmTHXXZ/6f
TLSH:	0BF73313BC4F7821D2A52D31873A5724C6216D414EE1B966B3A13EABFEF11C0EE64DD2
File Content Preview:	.....>..... ...$...(...,...0...4...8...<...@...D.....

File Icon

Icon Hash:	a2a0b496b2caca72

Network Behavior

No network behavior found

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 6044, Parent PID: 3324

General

Target ID:	0
Start time:	00:43:50
Start date:	24/11/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\PWMinderInstaller-3.3.1.1.msi"
Imagebase:	0x7ff6a6920000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6096**, Parent PID: **564**

General

Target ID:	1
Start time:	00:43:52
Start date:	24/11/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff6a6920000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	81193	94	31 31 2f 32 34 2f 32 30 32 32 20 30 30 3a 34 34 3a 32 31 2e 32 34 31 20 5b 36 30 39 36 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	11/24/2022 00:44:21.241 [6096]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFA059CBEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFA059CBBC6	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **1348**, Parent PID: **6096**

General

Target ID:	2
Start time:	00:44:05
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 483844CA7CD225D329998D5B1C5B7780 C
Imagebase:	0x1080000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msiexec.exe PID: **6048**, Parent PID: **6096**

General

Target ID:	3
Start time:	00:44:21
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding BD76792E804F7BE88D040374A60ADC55
Imagebase:	0x1080000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly