





The screenshot displays the Malwarebytes Anti-Malware application window during a scan. At the top, the status bar indicates "Malicious activity". The main header shows the file path "e204ea1ba265a360e22a3dcdad634806...", its MD5 hash "MD5: 6C47A3FE395BD041703B4C8AFC2F0AE4", and the scan details "Start: 21.10.2020, 03:47" and "Total time: 120 s". Below this, the operating system is identified as "Win7 32 bit Complete".

The "Indicators:" section shows several icons representing different types of indicators. A toolbar at the top right includes buttons for "Get sample", "IOC", "MalConf", "Restart", "Text report", "Graph", "ATT&CK", "AI Summary" (marked as beta), and "Export".

The central part of the interface features a "Processes" tab with a filter set to "Filter by PID or name". A checkbox labeled "Only important" is checked. The process list is displayed in a tree view, showing the following processes:

- explorer.exe** (PID 392, SUS) - Memory usage: 1k, CPU: 1k, Private bytes: 233.
- WinRAR.exe** (PID 2516) - Command line: "C:\Users\admin\AppData\Local\Temp\e204ea1...". Memory usage: 1k, CPU: 445, Private bytes: 180.
- mshta.exe** (PID 2068) - Command line: "https://rarebooksocietyofindia.org/utills/assets/le...". Memory usage: 1k, CPU: 560, Private bytes: 256.
- WScript.exe** (PID 1144) - Command line: "C:\ProgramData\update.js". Memory usage: 177, CPU: 14, Private bytes: 40.
- AcroRd32.exe** (PID 2512) - Command line: "C:\Users\admin\AppData\Local\Temp\ET...". Memory usage: 9k, CPU: 64, Private bytes: 176.
- AcroRd32.exe** (PID 680) - Command line: "--type=renderer C:\Users\admin\AppData...". Memory usage: 12k, CPU: 109, Private bytes: 186.
- RdrCEF.exe** (PID 3772) - Command line: "--backgroundcolor=16448250". Memory usage: 1k, CPU: 11, Private bytes: 132.
- RdrCEF.exe** (PID 3444) - Command line: "--type=renderer --disable-3d-apis --dis...". Memory usage: 335, CPU: 0, Private bytes: 104.
- RdrCEF.exe** (PID 2840) - Command line: "--type=renderer --disable-3d-apis --dis...". Memory usage: 275, CPU: 0, Private bytes: 104.
- mshta.exe** (PID 2084) - Command line: "https://rarebooksocietyofindia.org/utills/asset...". Memory usage: 1k, CPU: 234, Private bytes: 268.
- cmd.exe** (PID 3336) - Command line: "/c ""C:\ProgramData\Viewer\addreg.bat"" ". Memory usage: 149, CPU: 6, Private bytes: 32.
- reg.exe** (PID 1480) - Command line: "ADD \"HKCU\SOFTWARE\Microsoft\Wind...\"". Memory usage: 43, CPU: 1, Private bytes: 34.
- mshta.exe** (PID 2484) - Command line: "\"C:\ProgramData\Fedly\fedlytext.hta\"". Memory usage: 733, CPU: 172, Private bytes: 119.
- cmd.exe** (PID 2400) - Command line: "/c ""C:\ProgramData\Fedly\addreg.bat"" ". Memory usage: 151, CPU: 6, Private bytes: 32.
- reg.exe** (PID 3932) - Command line: "ADD \"HKCU\SOFTWARE\Microsoft\Wind...\"". Memory usage: 44, CPU: 1, Private bytes: 34.

▶		HTTP Requests	8	Connections	10	DNS Requests	6	Threats	0	Filter by PID, name or url	📄 PCAP
NETWORK	Timeshift	Headers			Rep	PID	Process name	CN	URL		Content
	24352 ms	GET   200: OK			?	392	explorer.exe		http://isrg.trustid.ocsp.identrust.com/...		1
	25350 ms	GET   200: OK			?	392	explorer.exe		http://ocsp.int-x3.letsencrypt.org/MFM...		52
FILES	45158 ms	GET   304: Not Modifi...			?	2512	AcroRd32.exe		http://acroipm2.adobe.com/15/rdr/EN...		
	45159 ms	GET   304: Not Modifi...			?	2512	AcroRd32.exe		http://acroipm2.adobe.com/15/rdr/EN...		
	45161 ms	GET   304: Not Modifi...			?	2512	AcroRd32.exe		http://acroipm2.adobe.com/15/rdr/EN...		
DEBUG	45161 ms	GET   304: Not Modifi...			?	2512	AcroRd32.exe		http://acroipm2.adobe.com/15/rdr/EN...		
	45163 ms	GET   200: OK			?	2512	AcroRd32.exe		http://ocsp.digicert.com/MFEWtZBNM...		47
	47201 ms	GET   200: OK			?	2512	AcroRd32.exe		http://acroipm2.adobe.com/15/rdr/EN...		10

-  Pricing
-  Contacts
-  FAQ
-  Sign In

Danger
[1480] reg.exe
 Changes the autorun value in the registry
 
[Try community version for free!](#)
[Register now](#)