Matanbuchus Triage Notes

Published: 2022-06-19 · Archived: 2026-04-05 22:47:35 UTC

```
/tmp/samples/55d329a13da236bec15c4c67686b809a2fbf5f6c9625b62d900ac22a7b729ba9.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/4b87f95c4477fc66c58b8e16a74f9c47217913cb4a78dc69f27a364a099acd90.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/0bdf1060b85ad55e73393eb0b59c1d226e091da4f4dcce65dacba5e9a1fd76a7.bin
[b'VirtualAlloc', b'start dll HackCheck', b'http://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/home.

/tmp/samples/3cae2ce9b2d7040292f1661af63dc28e778027c46f78d8be3b1d43f4b6c2b046.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/b4e7710488c2b7aaa71688b8bd546410af07a215c2e835e8dfbe24887186bd4f.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/orig.bin
[b'VirtualAlloc', b'start dll HackCheck', b'http://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/home.

/tmp/samples/2f36c571f20b2b2c2058d4db574a6d53b148450356bf529d72aefc19505c912e.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/4eb85a5532b98cbc4a6db1697cf46b9e2b7e28e89d6bbfc137b36c0736cd80e2.bin
[b'rundll32.exe\x00', b'ztCYGAuJ\x00', b'Shlwapi.dll\x00', b'WS2_32.dll\x00', b'https://windowsdrive

/tmp/samples/10d5483faf9a4e0fbc17556164f47f7014650797b7d501289b269515a0853b64.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/58a673023bbc7f2726e3b7ac917a43d9306692dc87b638ee21b98705a3262ccd.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/b9b399dbb5d901c16d97b7c30cc182736cd83a7c53313194a1798d61f9c7501e.bin
[]

/tmp/samples/fa6500946210334d397d612d5ee9b11456316e25672bc60c1267bbdb002af9c7.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/60f030597c75f9df0f7a494cb5432b600d41775cfe5cf13006c1448fa3a68d8d.bin
[b'VirtualAlloc', b'start dll HackCheck', b'http://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/home.

/tmp/samples/e58b9bbb7bcdf3e901453b7b9c9e514fed1e53565e3280353dccc77cde26a98e.bin
```

```
[b'C:\\Windows\\System32\\schtasks.exe\x00', b'rundll32.exe\x00', b' /TR "%windir%\\system32\\regsvr

/tmp/samples/a3c896e23c86e47bcb77096e743010546cd7699e0189344d11b9c642b89deef1.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x

/tmp/samples/f27821dddb17b6c8d59fb2ada1e90eac8d561476e5af3a6be064177683b0eee9.bin
[b'VirtualAlloc', b'Windows-Update-Agent/11.0.10011.16384 Client-Protocol/2.0\x00', b'rundll32.exe\x
```

Source: https://research.openanalysis.net/matanbuchus/loader/yara/triage/dumpulator/emulation/2022/06/19/matanbuchus-triage.html