

HITB2020: Voltron STA — The Lost Reports

Archived: 2026-04-05 13:30:42 UTC

In lieu of a proper write up, the following hashes should help replicate the work by any interested researchers. All samples discussed are available on VirusTotal :)

0xFancyFilter or Regin 1.5 ('htmlfiltxx64.dll' or 'Microsoft\Internet Explorer\iesrch32.dat')

- cd3ee807e349abae65d93e421176f302528b739e9e1d77a6ce4e57caeec91b4e

Older 0xFF samples ('httpfilt.dll', 'htmlfilt.dll')

- 369145c6f366f25a4e8878ad1ffec73d680cdc2da4380b221d1d7cdf3a90c930
- ef35705696d78cc9f4de6adad2cbe5ed22fd50da0ce4180c1d47cf0536aebc87
- df4bc387181ffaabe0be39e66ef5eb838ed638e0ae2b82e9a7daa83647e38bb1

Old EQGRP 'nethdlr' (MISTYVEAL) for comparison

- d8bab0b79bafec3a41db0dd4ae1703c2ab55de5af261e1881d62bde0d9033690

Regin's Hopscotch with shared RC4 implementation

- d83428779b0c0ebfa08c6b50f34e0f1ae7812eeb9ed78b86610517d8208b6cb3

YARA

- A broad YARA rule focused on 0xFF features is available [HERE](#)

Source: <https://www.epicturla.com/previous-works/hitb2020-voltron-sta>