LevelBlue - Open Threat Exchange

By Arek-BTC

Archived: 2026-04-05 15:45:26 UTC

sdfzsdf.ele fac1ec40eea5a4fc05f17e019328e287

FileHash-MD5: 28 | **FileHash-SHA1:** 27 | **FileHash-SHA256:** 1077 | **URL:** 1092 | **YARA:** 535 | **Domain:** 282 | **Email:** 4 | **Hostname:** 316

SHA1- 33008f85428a83996083c3da92a8f00595071403 SHA256 cdab1c3196887d4f749d82f014786a966c87f35a7189f0f3d078558b957847bf
https://sandbox.ti.qianxin.com/sandbox/page/detail?type=file&id=7b6726e20c513baebf7fd387a3dd1b7d67a4c7c4
https://ti.qianxin.com/v2/search?type=file&value=fac1ec40eea5a4fc05f17e019328e287
https://www.virustotal.com/gui/file/cdab1c3196887d4f749d82f014786a966c87f35a7189f0f3d078558b957847bf/relations

- 122 Subscribers

dfirfanatic_IOC's

CVE: 11 | **FileHash-MD5:** 3 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 6 | **URL:** 20 | **Domain:** 39 | **Hostname:** 12

51.15.98.45 51.15.115.141 51.15.44.6 107.23.39.208 154.38.185.108 139.59.30.78 139.59.30.78 141.98.11.168 195.164.49.68 152.39.227.27 212.56.53.90 159.65.231.167 195.154.208.101 195.154.208.99 163.172.77.100 47.84.83.221 104.28.211.187 152.42.211.173 174.138.17.185 209.146.60.235 45.9.148.131 2a0e:fa00:0:25::1 178.128.208.31 157.66.55.50 178.128.208.31 104.28.211.187 13.76.244.181 201.46.112.135 118.41.203.50 51.75.126.7 188.166.163.12 195.242.212.198 93.123.109.246 152.32.129.236

- 1 Subscribers

- 161 Subscribers

APT36 - In the Wake of Pahalgam Attack & Operation Sindhoor

CVE: 1 | **FileHash-MD5:** 31 | **FileHash-SHA1:** 29 | **FileHash-SHA256:** 31 | **URL:** 23 | **Domain:** 28 | **Email:** 1 | **Hostname:** 25

This is a collection of IOCs, I was able to collect from various sources which are related to the recent India-Pakistan clashes and cyber operations taking place.

- 50 Subscribers

PolymodXT.exe

FileHash-MD5: 414 | **FileHash-SHA1:** 410 | **FileHash-SHA256:** 1940 | **URL:** 171 | **YARA:** 759 | **Domain:** 134 | **Email:** 4 | **Hostname:** 56

- 122 Subscribers

Svchost id: 16c37b52-b141-42a5-a3ea-bbe098444397

FileHash-MD5: 39 | **FileHash-SHA1:** 28 | **FileHash-SHA256:** 1065 | **URL:** 984 | **YARA:** 535 | **Domain:** 262 | **Email:** 4 | **Hostname:** 316

The following rules for the Windows.Trojan.Tofsee malware have been revealed by the BBC's Panorama programme and are subject to a review by BBC Newsnight and BBC Radio 5 live.

- 122 Subscribers

Snowblind: The Invisible Hand of Secret Blizzard

A Russian-based threat actor, Secret Blizzard, has infiltrated 33 command-and-control nodes of a Pakistani-based actor, Storm-0156. Over two years, Secret Blizzard leveraged this access to deploy malware into Afghan government networks and potentially acquired data from Pakistani operators' workstations. They expanded their focus to include two other malware families, Waiscot and CrimsonRAT, used against Indian targets. The campaign demonstrates Secret Blizzard's meticulous approach to expanding operations in the Middle East, exploiting other actors' infrastructure to avoid attribution and gain sensitive information. This strategy allows them to remotely acquire data without exposing their own tools, taking advantage of the foothold created by the original threat actor.

- 373,939 Subscribers

- 35 Subscribers

Author Url

- 841 Subscribers

- 181 Subscribers

- 258 Subscribers

VajraSpy RAT IOCs - SEC-1275-1

FileHash-MD5: 8 | **FileHash-SHA1:** 13 | **FileHash-SHA256:** 8

Search for the VajraSpy RAT IOCs, Â£1.2m, on Google's Android platform, and on the Google Play app, as well as for ESET.

- 34 Subscribers

- 41 Subscribers

Author Url

- 841 Subscribers

Author Url

- 841 Subscribers

CapraTube | Transparent Tribe’s CapraRAT Mimics YouTube to Hijack Android Phones

FileHash-MD5: 2 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 2 | **Domain:** 3

Transparent Tribe is a suspected Pakistani actor known for targeting military and diplomatic personnel in both India and Pakistan, with a more recent expansion to the Indian Education sector. Since 2018, reports have detailed the group’s use of what is now called CapraRAT, an Android framework that hides RAT features inside of another application. The toolset has been used for surveillance against spear-phishing targets privy to affairs involving the disputed region of Kashmir, as well as human rights activists working on matters related to Pakistan.

- 373,939 Subscribers

Author Url

- 841 Subscribers

- 258 Subscribers

- 181 Subscribers

- 181 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:CrimsonRAT