Crimson RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:23:25 UTC

It was first discovered in 2017 and has since been used to attack organizations around the world. The malware is often distributed through phishing emails or by exploiting vulnerabilities in outdated security software. Once Crimson RAT is installed on a computer, it can be used to steal data, spy on users, and even take control of the infected computers.

Remote control of infected computers
Data theft, such as passwords, files, and emails
User spying
Takeover of infected computers
Locking of infected computers
Extortion of payments

2025-04-30 · Seqrite ·
Advisory: Pahalgam Attack themed decoys used by APT36 to target the Indian Government
Crimson RAT 2024-12-04 · Lumen · Black Lotus Labs, Danny Adamitis, Ryan English
Snowblind: The Invisible Hand of Secret Blizzard
Crimson RAT TwoDash 2024-12-04 · Microsoft · Microsoft Threat Intelligence
Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage
Crimson RAT MiniPocket TwoDash Wainscot Operation C-Major Storm-0473 2024-07-23 · K7 Security · Dhanush
Threat actors target recent Election Results
Crimson RAT 2024-04-24 · Seqrite · Sathwik Ram Prakki
Pakistani APTs Escalate Attacks on Indian Gov. Seqrite Labs Unveils Threats and Connections
AllaKore Crimson RAT 2023-10-12 · Cluster25 · Cluster25 Threat Intel Team
CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations
Agent Tesla Crimson RAT Nanocore RAT SmokeLoader 2023-07-13 · Brandefense · Brandefense
APT 36 Campaign – Poseidon Malware Technical Analysis
Poseidon Crimson RAT Oblique RAT 2023-05-02 · Seqrite · Sathwik Ram Prakki
Transparent Tribe APT actively lures Indian Army amidst increased targeting of Educational Institutions
Crimson RAT 2022-08-12 · Brandefense · Brandefense
Mythic Leopard APT Group
Crimson RAT DarkComet NjRAT Oblique RAT Peppy RAT 2022-07-13 · Cisco · Nick Biasini
Transparent Tribe begins targeting education sector in latest campaign
Crimson RAT Oblique RAT 2022-05-11 · K7 Security · Saikumaravel
Transparent Tribe Targets Educational Institution
Crimson RAT 2022-03-29 · Cisco Talos · Asheer Malhotra, Justin Thattil, Kendall McKay

Transparent Tribe campaign uses new bespoke malware to target Indian government officials

Crimson RAT 2022-03-29 · Bleeping Computer · Bill Toulas

Hackers use modified MFA tool against Indian govt employees

Crimson RAT Oblique RAT 2022-03-10 · Twitter (@Katechondic) · Katechondic

Tweet on additional computer names "desktop-g1i8n3f" & "desktop-j6llo2k", seen with Crimson RAT C2 infrastructure used by APT36

Crimson RAT 2022-03-10 · Twitter (@teamcymru_S2) · Team Cymru

Tweet on Crimson RAT infrastructure used by APT36

Crimson RAT 2022-01-24 · Trend Micro · Trend Micro

Investigating APT36 or Earth Karkaddan’s Attack Chain and Malware Arsenal

CapraRAT Crimson RAT Oblique RAT Operation C-Major 2022-01-24 · Trend Micro · Trend Micro

Investigating APT36 or Earth Karkaddan’s Attack Chain and Malware Arsenal (IOCs)

Crimson RAT Oblique RAT 2022-01-24 · Trend Micro · Trend Micro

Investigating APT36 or Earth Karkaddan’s Attack Chain and Malware Arsenal

Crimson RAT Oblique RAT 2021-12-22 · Know Chuangyu · Know Chuangyu

APT Tracking Analytics: Transparent Tribe Attack Activity

Crimson RAT 2021-10-13 · Anchored Narratives on Threat Intelligence and Geopolitics · RJM

Trouble in Asia and the Middle East. Tracking the TransparentTribe threat actor.

Crimson RAT 2021-09-08 · · Microstep Intelligence Bureau · Microstep Online Research Response Center

Trilateral operation: years of cyberespionage against countries in south asia and the middle east (APT36)

AndroRAT Crimson RAT 2021-09-01 · · 360 Threat Intelligence Center · Advanced Threat Institute

APT-C-56 (Transparent Tribe) Latest Attack Analysis and Associated Suspected Gorgon Group Attack Analysis Alert

Crimson RAT NetWire RC 2021-07-02 · Team Cymru · Joshua Picolet

Transparent Tribe APT Infrastructure Mapping Part 2: A Deeper Dive into the Identification of CrimsonRAT Infrastructure

Crimson RAT 2021-05-13 · Talos · Asheer Malhotra, Justin Thattil, Kendall McKay

Transparent Tribe APT expands its Windows malware arsenal

Crimson RAT Oblique RAT 2021-05-05 · Zscaler · Aniruddha Dolas, Manohar Ghule, Mohd Sadique

Catching RATs Over Custom Protocols Analysis of top non-HTTP/S threats

Agent Tesla AsyncRAT Crimson RAT CyberGate Ghost RAT Nanocore RAT NetWire RC NjRAT Quasar RAT Remcos 2021-04-30 · Cybleinc · cybleinc

Transparent Tribe Operating with a New Variant of Crimson RAT

Crimson RAT 2021-04-20 · · 360 Threat Intelligence Center · Advanced Threat Institute

Transparent Tribe uses the new crown vaccine hotspot to analyze the targeted attacks on the Indian medical industry

Crimson RAT 2021-04-16 · Team Cymru · Joshua Picolet

Transparent Tribe APT Infrastructure Mapping Part 1: A High-Level Study of CrimsonRAT Infrastructure October 2020 – March 2021

Crimson RAT 2021-02-28 · PWC UK · PWC UK

Cyber Threats 2020: A Year in Retrospect

elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot

BazarBackdoor BLINDINGCAN Chinoxy Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team 2021-01-18 · Twitter (@teamcymru) · Team Cymru

Tweet on APT36 CrimsonRAT C2

Crimson RAT 2020-11-03 · Kaspersky Labs · GReAT

APT trends report Q3 2020

WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti 2020-08-26 · Kaspersky Labs · Giampaolo Dedola

Transparent Tribe: Evolution analysis, part 2

AhMyth Crimson RAT Oblique RAT 2020-08-25 · · Qianxin · Qi'anxin Threat Intelligence

南亚APT组织“透明部落”在移动端上与对手的较量

AhMyth Crimson RAT Oblique RAT 2020-08-20 · Kaspersky Labs · Giampaolo Dedola

Transparent Tribe: Evolution analysis, part 1

Crimson RAT 2020-07-08 · Seqrite · Kalpesh Mantri

Operation ‘Honey Trap’: APT36 Targets Defense Organizations in India

Crimson RAT 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-02-21 · Yoroi · Antonio Pirozzi, Luigi Martire, Pietro Melillo

Transparent Tribe: Four Years Later

Crimson RAT 2020-01-01 · Secureworks · SecureWorks

COPPER FIELDSTONE

Crimson RAT DarkComet Luminosity RAT NjRAT Operation C-Major 2019-09-26 · Proofpoint · Bryan Campbell, Jeremy Hedges, Proofpoint Threat Insight Team

New WhiteShadow downloader uses Microsoft SQL to retrieve malware

WhiteShadow Agent Tesla Azorult Crimson RAT Formbook Nanocore RAT NetWire RC NjRAT Remcos 2019-03-05 · · Tencent · Tencent

TransparentTribe APT organizes 2019 attacks on Indian government and military targets

Crimson RAT Unidentified 066 Operation C-Major 2018-05-15 · Amnesty International · Brave

HUMAN RIGHTS UNDER SURVEILLANCE DIGITAL THREATS AGAINST HUMAN RIGHTS DEFENDERS IN PAKISTAN

StealthAgent Crimson RAT 2016-03-01 · Proofpoint · Darien Huss

Operation Transparent Tribe

Andromeda beendoor Bezigate Crimson RAT Luminosity RAT Operation C-Major

▶ [TLP:WHITE] win_crimson_auto (20180607 | autogenerated rule brought to you by yara-signator)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.crimson