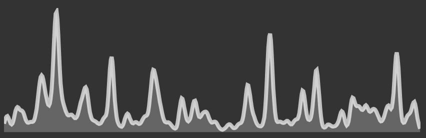
THREAT ACTOR

Storm-1567

35 mentions in the last 2 weeks



1K articles in the last 12 months

Using open-source data collected by Feedly AI.

Overview

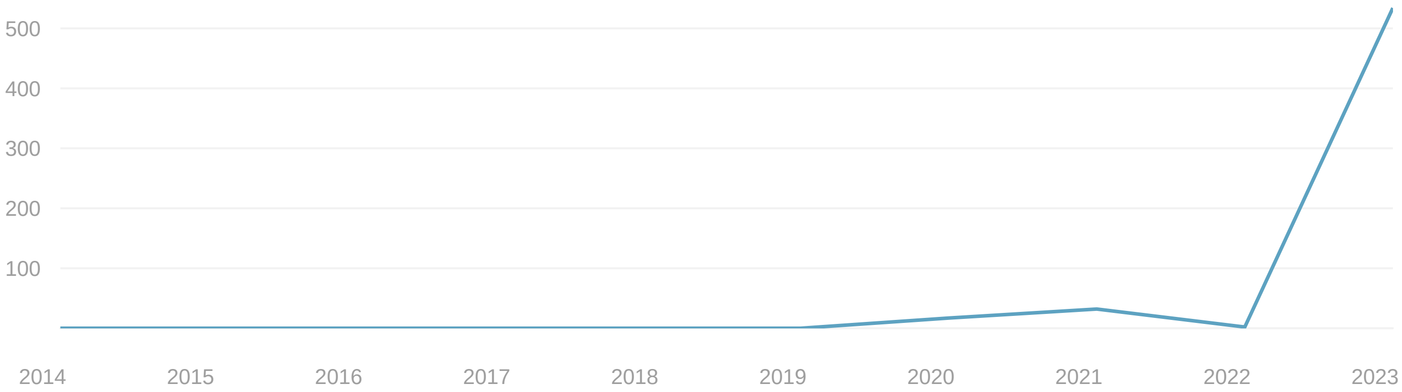
Storm-1567 is a ransomware group that emerged in March 2023, operating under a Ransomware-as-a-Service (RaaS) model. It has been linked to the Conti ransomware group due to code similarities and shared tactics, techniques, and procedures (TTPs). Storm-1567 primarily targets organizations in North America, Europe, and Australia, impacting various sectors including manufacturing, technology, and cri...

See More

Aliases

- Akira
- GOLD SAHARA
- PUNK SPIDER

Article count



Targets

No targeted countries have been identified by MISP

Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED

No attack has been detected in the time frame selected

Top malware families associated with this threat actor

Loading...

Tactics, Techniques, and Procedures

Last mentioned

Loading...

Exploited vulnerabilities

Loading...

Detection Rules

RULE	ARTICLES	COUNT	ACTION
YARA rules	1	1	Download

Threat intelligence reports

Threat Assessment: Howling Scorpius (Akira Ransomware)

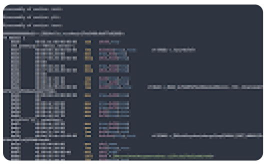
AI Threat Actors • by Yoav Zemah / 5d • Threat Actors • Threat Intelligence Reports • 2 CVEs

submitted by /u/jnazario [link] [comments]

Inside Akira Ransomware's Rust Experiment

Threat Actors • by benhe / 5d • Threat Intelligence Reports • 6 TTPs • Akira ransomware targets ESXi servers

submitted by /u/digicat [link] [comments]



Inside Akira Ransomware’s Rust Experiment

Threat Actors • Check Point Research by benhe / 6d • Threat Intelligence Reports • 5 TTPs

Broadly speaking, parses arguments, determines program behavior and collects targeted files, and is a wrapper that launches threads that carry out the actual encryption logic that lives in . So, first of all, they added code allowing the…

Also in Check Point Research, WizCase, +11 feeds

Observes Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN

CVE-2024-40766 • by digicat / 40d

submitted by /u/digicat [link] [comments]

Also in IT Security News, Cybersecurity News, +58 feeds

Akira ransomware continues to evolve

8 CVEs • Cisco Talos Blog by James Nutland / 49d • IoC > 37 hashes • 25 TTPs

1197801c36f73cff2fc88cecbe3d88d1a 3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30 Windows v1…

News

Black Basta Ransomware Evolves with Email Bombing, QR Codes, and Social Engineering

AI New Malware > Elpaco • 23 The Hacker News by info@thehackernews.com (The Hacker News) / 6h • 21 TTPs • Black Basta Ransomware evolves tactics

The threat actors linked to the Black Basta ransomware have been observed switching up their social engineering tactics, distributing a different set of payloads such as Zbot and DarkGate since early October 2024. Rapid7 said it also…

Also in The Hacker News | #1..., Talkback News, +28 feeds

[AKIRA] – Ransomware Victim: Consumers Builders Supply

Akira ransomware claims multiple victims • RedPacket Security by admin / 8h

The ransomware leak page for Consumers Builders Supply, a company operating in the construction industry in the United States, highlights a compromise involving internal corporate documents. This blog is simply posting an editorial…

Also in #ransomware, Ransomware.live Last..., +25 feeds

[AKIRA] – Ransomware Victim: Cipla

Akira ransomware claims multiple victims •

RedPacket Security by admin / 8h

The ransomware leak page pertaining to Cipla, a prominent player in the healthcare industry, outlines significant breaches involving internal corporate data. This blog is simply posting an editorial news post informing that a company has…

Also in #ransomware, Ransomware.live Last..., +23 feeds

[AKIRA] – Ransomware Victim: ECBM

Akira ransomware claims multiple victims •

RedPacket Security by admin / 8h

This blog is simply posting an editorial news post informing that a company has fallen victim to a ransomware attack. The ransomware leak page associated with ECBM, a family-owned independent insurance broker and consulting firm base…

Also in #ransomware, Ransomware.live Last..., +23 feeds

Cipla Allegedly Hacked, Akira Ransomware Claims 70GB Data Stolen

Akira ransomware claims multiple victims •

Cyber Security News by Guru Baran / 10h

According to the Akira ransomware group's claims, the stolen information includes a wide range of sensitive data: Cipla, the Indian pharmaceutical giant, has reportedly fallen victim to a cyberattack orchestrated by the Akira ransomware…

Also in #ransomware, Ransomware.live Last..., +27 feeds

9th December – Threat Intelligence Report

3 CVEs • Check Point Research by hagarb / 11h • 12 TTPs

Stoli Group USA has filed for Chapter 11 bankruptcy after an August 2024 ransomware attack severely disrupted its IT infrastructure, forcing manual operations and hindering financial reporting. ENGlobal Corporation, an energy…

See 44 more articles and social media posts

Made with feedly