# **Analysis Overview** ▲Request Report Deletion Submission name: ransomware\_c2.exe Size: 3.2MiB Type: peexe (/search?query=filetype:peexe&block\_redirect=1) 64bits (/search?query=filetype:64bits&block\_redirect=1) executable (/search?query=filetype:executable&block\_redirect=1) 🚯 Mime: application/vnd.microsoft.portable-executable SHA256: dc40d6f0cb069d6b89ba4742d4601fbb8186330168fb53111797932df5488972 (/search? **Submitted At:** 2025-06-20 11:57:19 (UTC) Last Anti-Virus Scan: 2025-06-20 11:57:21 (UTC) **Last Sandbox Report:** 2025-06-20 11:57:19 (UTC) suspicious Threat Score: 61/100 AV Detection: 2% Labeled As: Ransom/Cerber.t (/search?query=vxfamily%3A"Ransom/Cerber.t") X Post (/sample-overview/dc40d6f0cb069d6b89ba4742d4601fbb8186330168fb53111797932df5488972/share/twitter) **⊘**Link 😝 E-Mail 0 Community Score 1 0 Anti-Virus Results ✓ Updated a while ago



MetaDefender Multi Scan Analysis

(https://www.opswat.com/metadefender-co utm\_campaign=Technology%%20Partners&utm\_sou



Malicious (1/27)

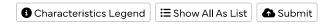
**₼** More Details

You don't have a malware problem, you have an adversary problem. CrowdStrike combines human analysis with a technical data collection platform to provide threat insights and expose the motivation, intent, TTPs for over 160 identified threat actors and numerous unnamed groups.

Learn more (https://www.crowdstrike.com/)

CrowdStrike Intelligence Blog (https://www.crowdstrike.com/blog/category/threat-intel-research/)

## Falcon Sandbox Reports (1)



**■** Windows 10 64 bit

#### ransomware\_c2.exe

June 20th 2025 11:57:19 (UTC)



### Suspicious

**Threat Score:** 

61/100

Indicators:

17 85

Labeled As:

Ransom/Cerber.t

Characteristics:



# **★** Falcon Sandbox Technology

#### **Hybrid Analysis: Powered by Falcon Sandbox**

Upgrade to a Falcon Sandbox license and gain full access to all features, IOCs and behavior analysis reportsData.

#### **Easily Deploy and Scale**

Process up to 25,000 files per month with Falcon Sandbox; because it is delivered on the cloud-native Falcon Platform, Falcon Sandbox is operational on Day One.

#### **Extensive Coverage**

Expanded support for file types and host operating systems.

Learn More! (https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/)

# Community

• There are no community comments.

• You must be logged in (/login) to submit a comment.

© 2025 Hybrid Analysis (https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/) — Hybrid Analysis Terms and Conditions of Use (/terms) — Hybrid Analysis Privacy Notice (/data-protection-policy) — Site Notice (/imprint) — Your Privacy Choices — Contact Us

# (https://twitter.com/HybridAnalysis)