

REvil Ransomware

Targeting the Kaseya VSA Vulnerability

<https://en.wikipedia.org/wiki/Revil>

A recent high profile exploit involving Kaseya VSA product was linked to the REvil ransomware. This report summarizes the Fortinet Security Fabric coverage for the REvil ransomware itself. Refer to the separate report for more detail about the Kaseya vulnerability.

Background

Kaseya is a high profile outbreak, with information still pending to be released regarding the initial vulnerability that was compromised. REvil is a known ransomware group/family that has been used in the past, and is part of existing security coverage by multiple Fortinet security products. Recently, it has been used by attackers targeting the high profile Kaseya VSA vulnerability, to demand ransom from many global organizations including MSPs who represent many hundred or thousand customers underneath. This report focusses specifically on the REvil ransomware protection and IOC detections by the Security Fabric products.

Announced

July 5: REvil ransomware gang takes credit for the Kaseya attack -

<https://gizmodo.com/revil-gang-takes-credit-for-massive-kaseya-attack-and-a-1847232663>

Latest Developments

Refer to the Kaseya timeline for the latest status of the on-premise patch and restoration of their SaaS service:

<https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689>

Fortinet Products

Summary

Services

Version

Other Info

FortiGate	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiClient	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiEDR	AV (Pre-Filter)	87.00359	FortiGuard AV detects the REvil payloads and file extractor
	EDR	v4+	FortiEDR can be used to effectively detect and mitigate post-exploitation activity associated with this threat.
FortiSandbox	AV (Pre-Filter)	87.00359	FortiGuard AV detects the REvil payloads and file extractor
	Behavior Detection	3.2.2+	FortiSandbox detects ransomware behaviors of the samples
FortiAI	AV (Pre-Filter)	87.00359	FortiGuard AV detects the REvil payloads and file extractor
	ANN	1.077	Artificial Neural Networks (ANN) Engine detects the known hashes
FortiMail	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiCASB	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiCWP	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiADC	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiProxy	AV	87.00359	FortiGuard AV detects the REvil payloads and file extractor
FortiAnalyzer	IOC	0.01915	FortiGuard IOC detects past log-based events accessing knowing C&C IPs and domains
	Event Handlers & Reports	6.2+	Detects indicators attributed to REvil from Fabric products.
FortiSIEM	IOC	0.01915	FortiGuard IOC detects past log-based events accessing knowing C&C IPs and domains
	Rules & Reports	6.2+	Detects indicators attributed to REvil from Fabric products and 3rd party products.
FortiClient/EMS	ZTNA Auto Tagging	6.4+	Detect and tag endpoints that are suspected compromised by the REvil ransomware

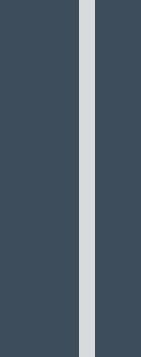
Cyber Kill Chain



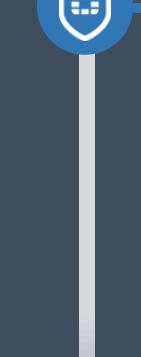
Reconnaissance



Weaponization



Delivery



FortiGate

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>



FortiClient

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>



FortiEDR

AV (Pre-Filter)

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>



FortiSandbox

AV (Pre-Filter)

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiAI

AV (Pre-Filter)

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiMail

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiCASB

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiCWP

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiADC

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiProxy

AV

Version Info: 87.00359

Link: <https://www.fortiguard.com/encyclopedia/virus/10039110>

FortiAnalyzer

IOC

Version Info: 0.01915

Link: <https://www.fortiguard.com/updates/ioc>

FortiSIEM

IOC

Version Info: 0.01915

Link: <https://www.fortiguard.com/updates/ioc>

FortiClient/EMS

ZTNA Auto Tagging

Version Info: 6.4+

Link: <https://www.fortiguard.com/updates/ztna-autotagging>

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response.

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer

IOC

Version Info: 0.01915

Link: <https://www.fortiguard.com/updates/ioc>

FortiSIEM

IOC

Version Info: 0.01915

Link: <https://www.fortiguard.com/updates/ioc>

FortiClient/EMS

ZTNA Auto Tagging

Version Info: 6.4+

Link: <https://www.fortiguard.com/updates/ztna-autotagging>

C2

Action

Endpoint