

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>

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

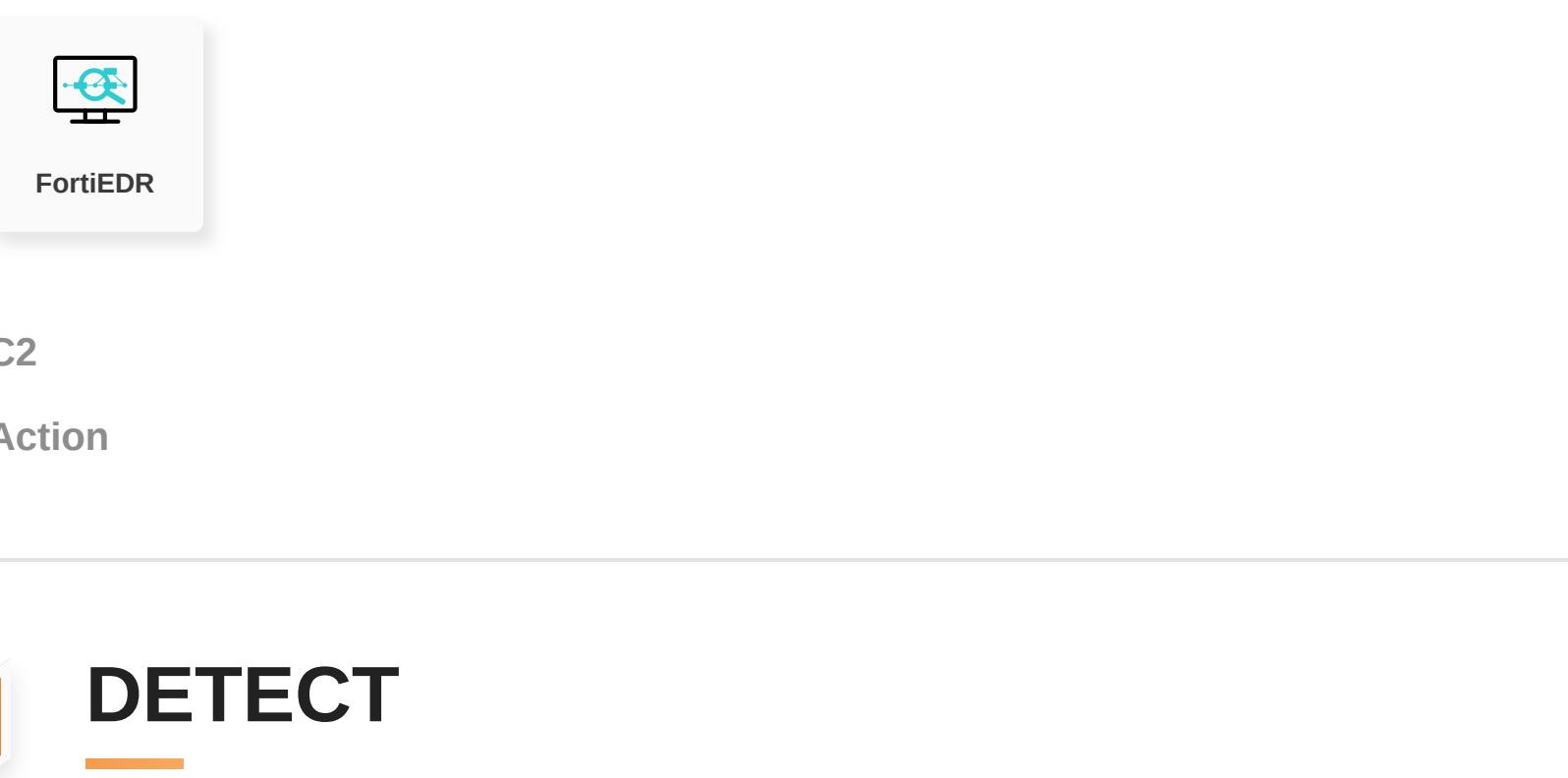
Reconnaissance

Weaponization

Delivery

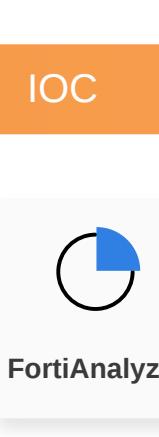
AV

FortiGuard AV detects the REvil payloads and file extractor



AV (Pre-filter)

FortiGuard AV detects the REvil payloads and file extractor



Behavior Detection

FortiSandbox detects ransomware behaviors of the samples



Exploitation

Installation

Post-execution

FortiEDR can be used to effectively detect and mitigate post-exploitation activity associated with this threat.



C2

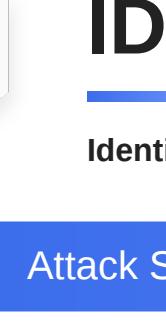
Action

DETECT

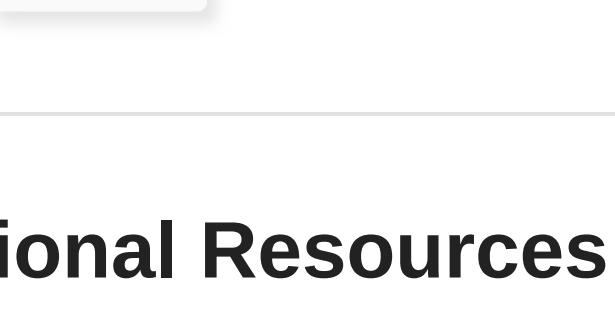
Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

Detect and tag endpoints that are suspected compromised by the REvil ransomware



IOC



Threat Hunting



RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

Experts to assist you with analysis, containment and response activities.



RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Additional Resources

Medium.com

<https://medium.com/@prateek.baghela/ransomware-attacks-analyzing-recent-high-profile-incidents-and-their-implications-8692ac9aefca>

Learn more about [FortiGuard Outbreak Alerts](#)