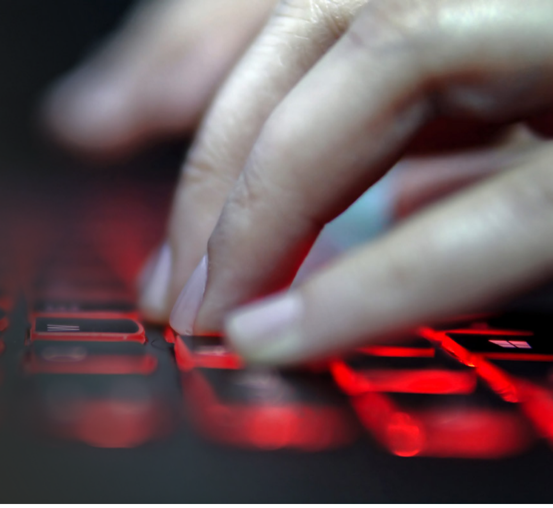


The REvil Ransomware Attack Against Kaseya Supply Chain: How Dark Cubed Can Help.

The Remote Monitoring and Management (RMM) platform, Kaseya, is widely used among Managed Service Providers (MSPs) and fell prey to a ransomware attack as reported on July 2, 2021. The attack began around 10:30 am EDT on July 2nd when attackers gained access to compromised Kaseya Virtual System Administration (VSA) servers which allow for remote management of customer infrastructure. The attackers uploaded malicious software packages to the VSA servers and leveraged their distribution capabilities to push the malware to multiple downstream destinations disguised as a Kaseya update. Upon arrival, these packages deployed ransomware which encrypted the datastores it had access to, then deleted the logfiles which would normally record this activity so as to obfuscate the sequence of events and delay or altogether prevent detection and attribution of the attack[1][2].

Affect on Dark Cubed Customers & Taking Action

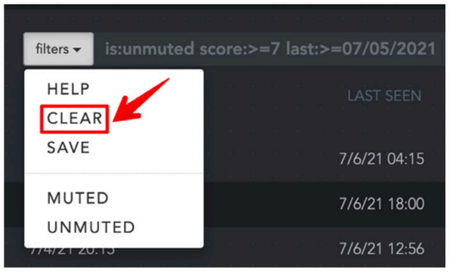
At the time of writing this article, no activity associated with these IOCs has been observed within Dark Cubed's commercial customer community. The VSAs which would be affected by the breach would be hosted on-premise within the MSP's network and accessible to the external internet. Best practices suggest that such infrastructure be hosted behind the network firewall to ensure access is limited to only legitimate users. Dark Cubed's MSP users whose VSAs are behind a Dark3-protected firewall will be able to detect activity related to these IOCs should they be affected. There are two areas where Dark Cubed users can take action: historical data analysis and automated threat notifications.

Historical Analysis

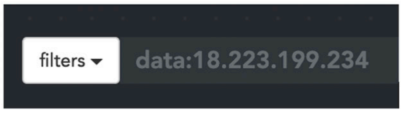
Within the Dark Cubed UI, a user can search for activity associated with a specific endpoint by leveraging the filter function of the Threat Data Table. Once on the page, expand the filters drop-down menu and select **CLEAR** to remove the default filter and display all data for the account. Next, enter a filter like the one shown below for each of the IOCs to determine if Dark Cubed has observed activity associated with those endpoints. The filter will start with 'data:' followed by the IP address without any spaces. Hit Enter or Return on your keyboard to display any relevant results.

Ideally, this filter will return a blank page for each of the IOCs queried. Should you see results populate after executing the filter, click into the entry shown in the Threat Data Table to gather more information and take action on the endpoint.

```
data:18.223.199.234
```



is:unmuted score:>=7 last:>=07/05/2021

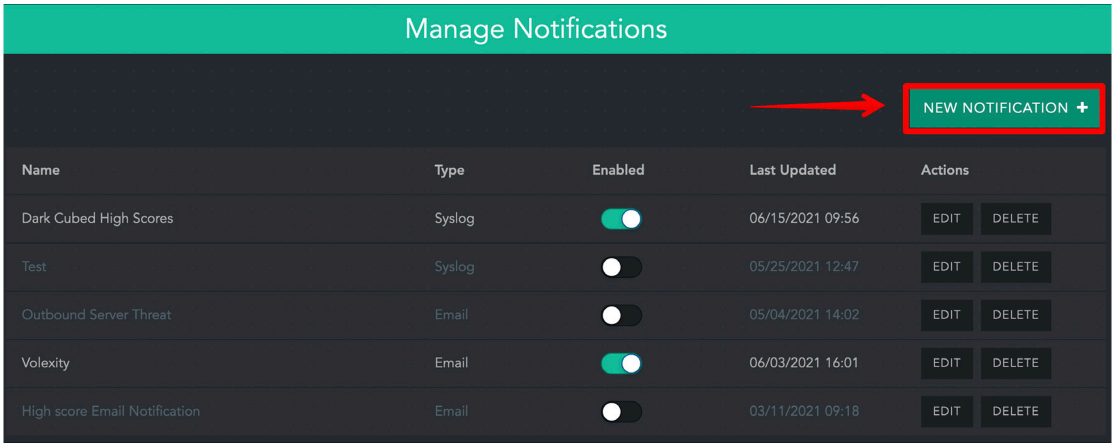


data:18.223.199.234

Automated Threat Notifications

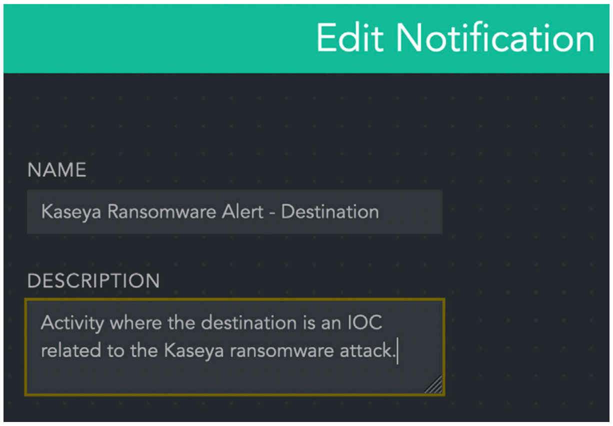
Dark Cubed recommends leveraging our advanced notification criteria to generate alerts upon activity associated with the endpoints implemented in the ransomware attack. Within the Dark Cubed UI, users can navigate to the notification configuration page and follow the steps below:

1 Start a new notification policy



Name	Type	Enabled	Last Updated	Actions
Dark Cubed High Scores	Syslog	●	06/15/2021 09:56	EDIT DELETE
Test	Syslog	○	05/25/2021 12:47	EDIT DELETE
Outbound Server Threat	Email	○	05/04/2021 14:02	EDIT DELETE
Volexity	Email	●	06/03/2021 16:01	EDIT DELETE
High score Email Notification	Email	○	03/11/2021 09:18	EDIT DELETE

2 Name the notification policy and provide a description



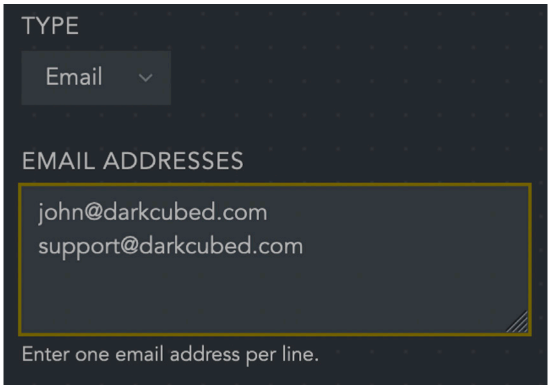
NAME

Kaseya Ransomware Alert - Destination

DESCRIPTION

Activity where the destination is an IOC related to the Kaseya ransomware attack.

3 Set your notification TYPE and the recipient(s). Notifications can be sent to email, Slack (or other webhook destination), or Syslog servers.



TYPE

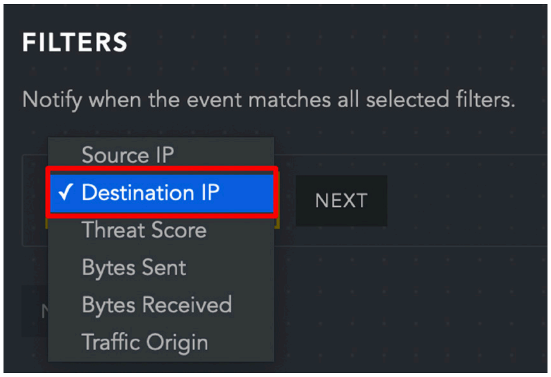
Email

EMAIL ADDRESSES

john@darkcubed.com
support@darkcubed.com

Enter one email address per line.

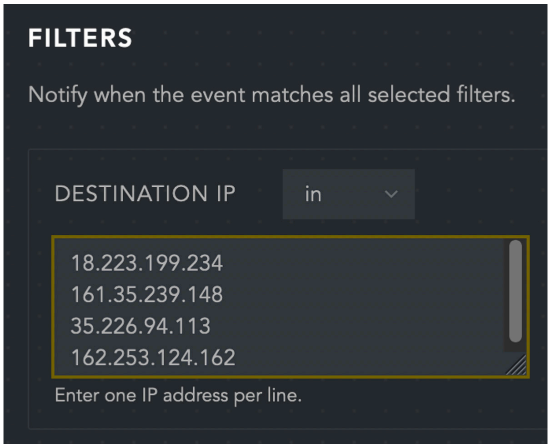
4 Under Filters, click **NEW FILTER** and select Destination IP from the drop-down menu.



FILTERS

Notify when the event matches all selected filters.

5 In the resulting dialog: ensure the DESTINATION IP qualifier is set to 'in' and enter the IP addresses as shown above.



FILTERS

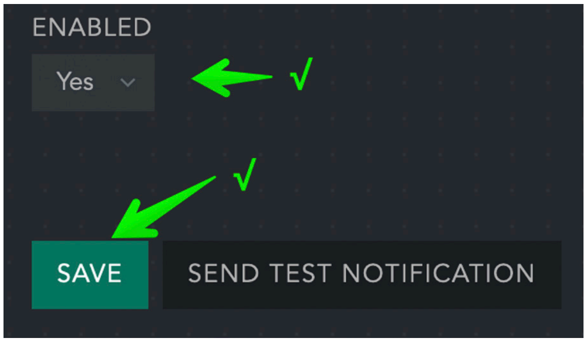
Notify when the event matches all selected filters.

DESTINATION IP in

18.223.199.234
161.35.239.148
35.226.94.113
162.253.124.162

Enter one IP address per line.

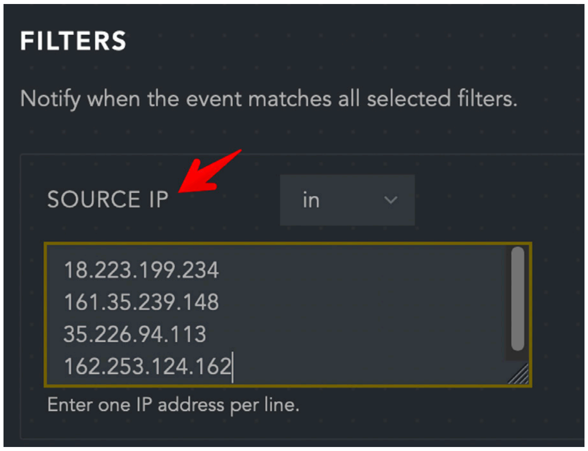
6 Ensure the policy is enabled and save your new configuration.



ENABLED

Yes

For full coverage, we recommend creating an additional notification policy following the same steps as above but where the IOCs are the SOURCE IP for the activity.



FILTERS

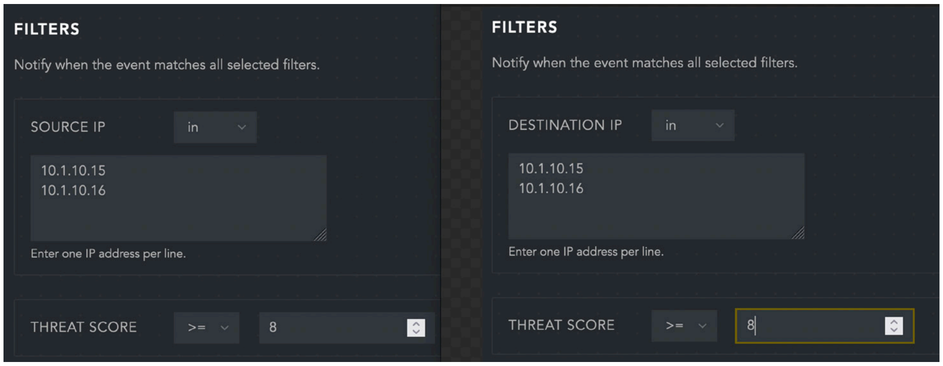
Notify when the event matches all selected filters.

SOURCE IP in

```
18.223.199.234
161.35.239.148
35.226.94.113
162.253.124.162
```

Enter one IP address per line.

MSP users may also find value in creating notification policies specific to their on-prem Kaseya infrastructure, as applicable, to identify other possible threats against those systems. In this case, follow the steps above, creating one policy with a SOURCE IP filter and one with a DESTINATION IP filter set to the private IP address(es) of the server(s) in question. These should each be paired with a THREAT SCORE filter set to ≥8 to alert upon high-threat activity associated with these endpoints that Dark Cubed considers potentially threatening.



FILTERS

Notify when the event matches all selected filters.

SOURCE IP in

```
10.1.10.15
10.1.10.16
```

Enter one IP address per line.

THREAT SCORE >= 8

FILTERS

Notify when the event matches all selected filters.

DESTINATION IP in

```
10.1.10.15
10.1.10.16
```

Enter one IP address per line.

THREAT SCORE >= 8

Further Recommendations & Resources

The Cybersecurity & Infrastructure Security Agency (CISA), in collaboration with the FBI, has established guidelines for MSPs to follow should they believe they are affected by the breach. Among these recommendations include using a tool published by Kaseya's security team to detect whether Indicators of Compromise (IoCs) were observed within the MSP's Kaseya environment[3]. Dark Cubed recommends taking this action as well, regardless of the presence or absence of IOC activity and related alerts generated within your Dark Cubed platform - as in some cases, the Kaseya infrastructure which is at risk could be located outside the scope of Dark Cubed monitoring.

As the situation continues to develop and more information is gathered, Kaseya, CISA & FBI, Huntress, and other organizations analyzing the attack may publish more guidance and IOCs related to the ransomware attack. Dark Cubed will also continue to track these indicators against its customer community and notify respective organizations should activity be observed in their network traffic. The resources Dark Cubed is using in this regard are listed in the footnote at the end of this article, along with current known IOCs; Dark Cubed recommends regularly checking these resources for updates. Our users are welcome to contact support@darkcubed.com for guidance in using this platform in relation to this attack.

Indicators of Compromise[1][4]

Users can search for activity in their Dark3 account using the 'data:' filter with the IOCs listed below (brackets are inserted for security and should be removed when using the IP address to search in the Dark3 UI).

18.223.199[.]234	(Amazon Web Services) discovered by Huntress
161.35.239[.]14	(Digital Ocean) discovered by TrueSec
35.226.94[.]113	(Google Cloud) discovered by Kaseya
162.253.124[.]162	(Sapioterra) discovered by Kaseya

Sources

[1] https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/

[2] https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021

[3] https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

[4] https://github.com/pgl/kaseya-revil-cnc-domains/blob/main/revil-kaseya-cnc-domains.txt

ABOUT DARK CUBED

Built from the bottom up for SMBs, the Dark Cubed SaaS solution augments existing firewalls to provide automated threat detection, scoring and blocking at a fraction of the cost and complexity of conventional cybersecurity products. We partner with MSPs and service providers to secure their customer bases, increase their revenue, and capture new customers. Founded by a former White House CISO, Dark Cubed is headquartered in Alexandria, VA.

www.darkcubed.com