[2]

2021

	APT !
	yuk-jo

1.
APT(advanced persistent threat) . APT , (Shipment Document), (P.O.–Purchase Order) . (Infostealer) 20201 2 . Content Disarm & Reconstruction(CDR) , ' & ' . Open source CDR ‘Dangerzone’ . , HWP . Gmail URL 1 Naver, Daum URL URL . APT URL Chrome extension . Chrome extension 2 , CDR URL ‘Dangerzone’ open source HWP ‘Dangerzone’ PDF VirusTotal API Naver, Daum URL .

2.

APT , CDR URL . , CDR URL .

CDR SaniTOX. SaniTOX . Web HWP, MS Office, PNG . , linux odt .

github CDR 'Dangerzone' . pixel flat PDF . docker 'Dangerzone' local machine HWP .

McAfee WebAdvisor block . , . Chrome extension . URL Naver, Daum URL .

CDR 'Dangerzone' Docker 'Dangerzone' , HWP .

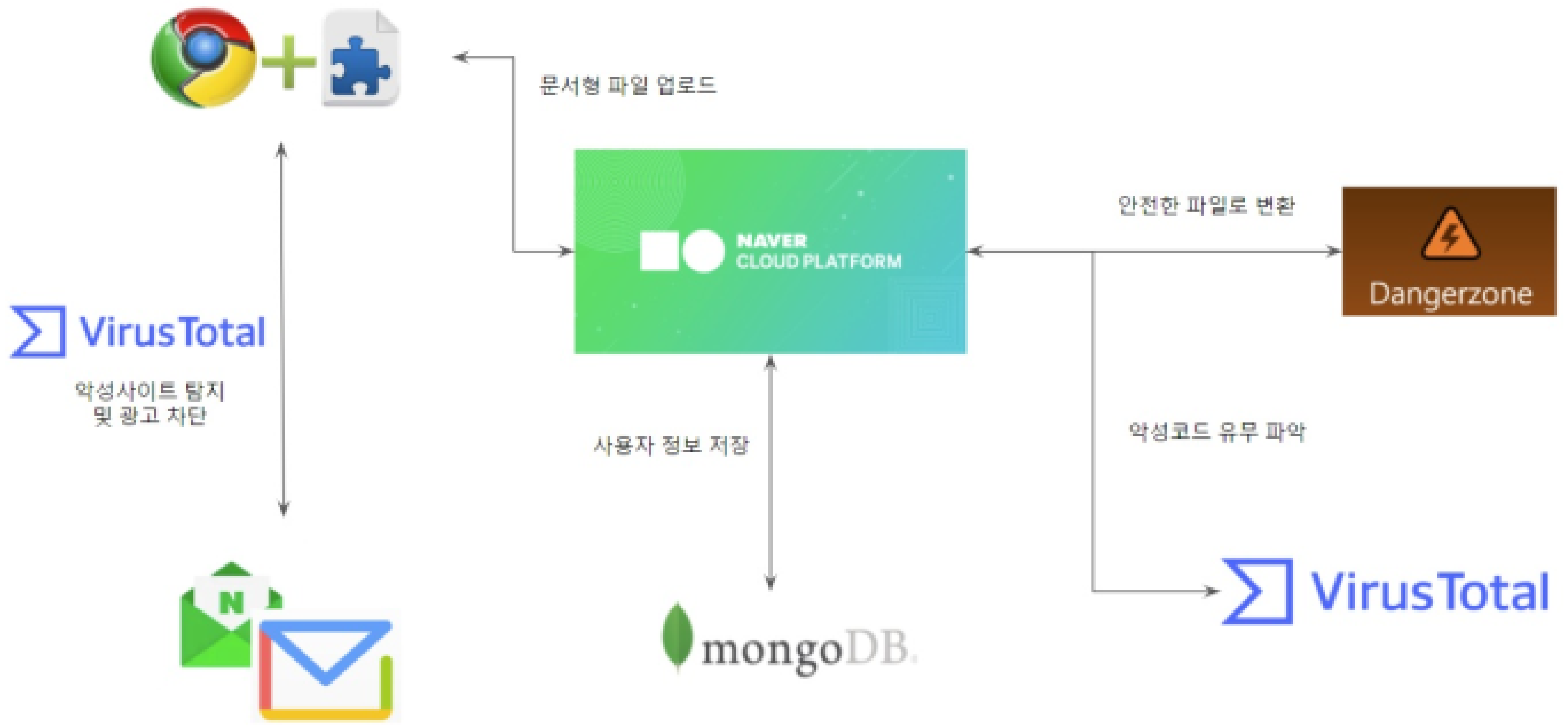
SaniTox web, cloud linux Open Document (odt, ods, odp, odg) .

McAfee WebAdvisor Chrome extension URL mail URL . Gmail Naver, Daum .

HWP CDR URL .

3.

1



3 . , MongoDB , mail URL .

Dangerzone Open source HWP docker container Naver Cloud Ubuntu server 18.04 LTS . CDR VirusTotal API .

MongoDB .

EasyList URL Chrome Extension API VirusTotal API Chrome Extension API URL .

Python pyhwp wkhtmltopdf HWP PDF . Chrome extension API VirusTotal API URL , Chrome extension . .

4.

. Dangerzone , chrome extension .

	()
	160,000
	400,000
	30,000
	590,000

, , . , HWP, Ms office , . Chrome extension .
APT .

§