Exposing Thousands of Active Kaseya Ransomware C&C Domains

Posted on September 23, 2021

About 1,500 small and medium-sized businesses (SMBs)[1] may have been affected by the ransomware attack targeting Kaseya, an IT solutions developer catering to managed service providers (MSPs) and enterprises. The attack, which occurred in July 2021, exploited a vulnerability in the company's remote monitoring and management software. The threat actors behind the attack reportedly asked for US$70 million[2] in exchange for a decryption tool.

Given the gravity of the attacks and the number of affected organizations, the security community can use as much threat intelligence as possible. To help both the security community and the exposed companies, WhoisXML API DNS Threat Researcher Dancho Danchev uncovered properties related to the Kaseya attacks and found several currently active.

Danchev prepared this report containing Kaseya ransomware indicators of compromise (IoCs) and artifacts, including:

- 1,200+ Kaseya command-and-control (C&C) server domains
- 40+ registrant email addresses believed to be involved in the campaign
- 200+ MD5 hashes involved in the campaign

Protecting against similar attacks is critical, especially for exposed companies. The IoCs and artifacts found in the report can provide technical details to help with cyber campaign attribution.

Get access to thousands of possible Internet properties related to the Kaseya ransomware attacks and learn how to uncover more on your own. Download the report now.

- [1] https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-

company-confirms/

- [2] https://www.zdnet.com/article/kaseya-ransomware-attack-us-launches-investigation-as-gang-demands-giant-70-million-payment/