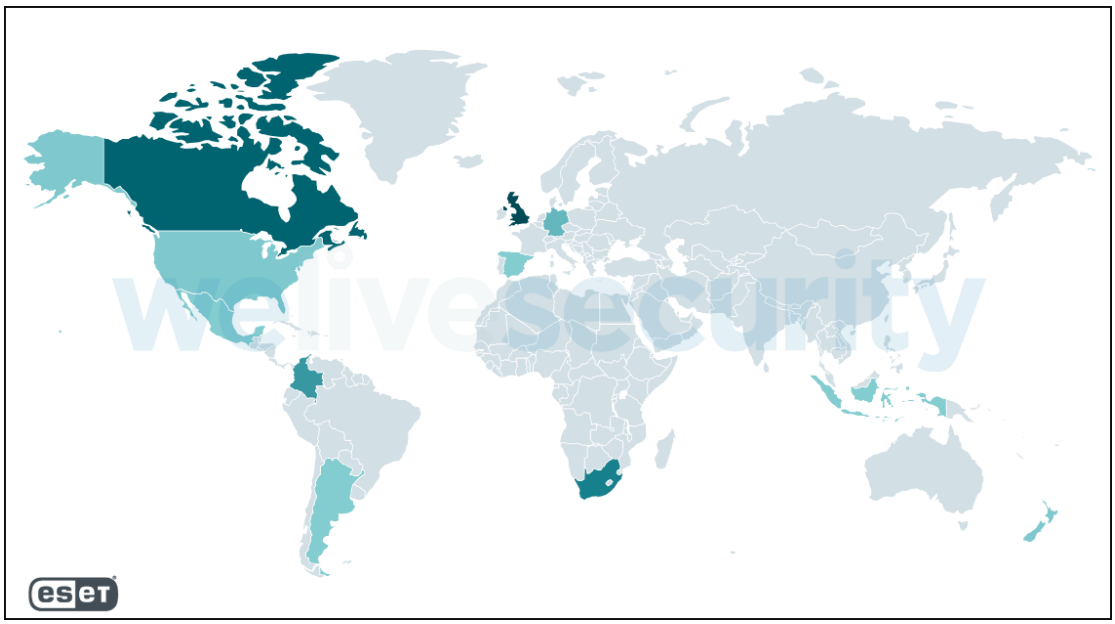
ESET Tech Center

Potential Kaseya VSA and MSP supply-chain attack

2021-07-07 - Steef | ESET Nederland - Comments (0) - Customer Advisories

As you may be aware, on July 2, 2021, Kaseya VSA, commonly used in Managed Service Provider (MSP) environments, was subject to a supply-chain ransomware attack. With parallels to December 2020's SolarWinds incident, this attack was reportedly delivered via an update of the Kaseya VSA software.

ESET products added the detection for this ransomware -Win32/Filecoder.Sodinokibi.N trojan- on July 2 at 9:22 PM CEST. This detection includes both the main executable of the ransomware, as well as Dynamic Link Library (DLL) files it side-loads. ESET telemetry shows the majority of reports coming from the United Kingdom, Canada, South Africa, Colombia, and Germany, followed by New Zealand, the United States, Argentina, Indonesia, Mexico, and Spain.



source: welivesecurity post

Kaseya began mitigation promptly on July2nd by notifying customers to immediately shut down their on-premises VSA servers. Past research into the Sodinokibi (aka REvil) criminal group highlights that the ransomware aims to shut down administrative access and begin encrypting data – prior to the full ransomware attack cycle.

While ESET and other vendors detect this malware, there was a lag between the time when the affected servers were hit and when support teams and security software could respond, allowing early infestations time to do damage. ESET is monitoring developments around the supply-chain attack, especially as concerns its systems. As a precaution, our engineers have taken the step to turn off our ERA and DEM plug-ins for Kaseya and will keep both on-premise and cloud servers turned off until further information can be confirmed about the attack's impact.

For further developments, please navigate to our ALERT here.