Threat Intelligence Report: Lazarus Group Campaign Targeting the Cryptocurrency Vertical

labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical/

In 2019, F-Secure uncovered technical details on Lazarus Group's modus operandi during an investigation of an attack on an organisation in the cryptocurrency vertical. Consistent with public reporting on the group's activities, the main objective of the attack was financial gain.

F-Secure assess the attack on the target to be advanced in nature and was able to link this activity with a global phishing campaign running since at least January 2018. The attack was linked to this wider set of activity through several common indicators found in samples from the investigation, open source repositories, and proprietary intelligence sources.

Lazarus Group's activities are a continued threat: the phishing campaign associated with this attack has been observed continuing into 2020, raising the need for awareness and ongoing vigilance amongst organisations operating in the targeted verticals. It is F-Secure's assessment that the group will continue to target organisations within the cryptocurrency vertical while it remains such a profitable pursuit, but may also expand to target supply chain elements of the vertical to increase returns and longevity of the campaign.

Where possible, evidence has been included in the body and appendices of this report to allow the security industry to leverage these details across their apertures, and draw their own conclusions. **F-Secure believes the detail in this report will help targeted organizations protect their networks from future attacks and raise the cost of operation for the group.**