Possible Master Key for REvil Posted on Github

flashpoint-intel.com/blog/possible-universal-revil-master-key-posted-to-xss/

August 10, 2021

Blogs

Blog

REvil Master Key for Kaseya Attack Posted to XSS

Flashpoint analysts have identified a post on the Russian language XSS Forum in which a threat actor operating under the alias of “Ekranoplan” posted a possible master key for REvil in a screenshot on Github.[1] Thus far, Flashpoint analysts have been able to attribute this key to restoration of data associated with the recent Kaseya ransomware attack, and are exploring whether there is broader applicability. exploring whether there is broader applicability.

Table Of Contents

Table of Contents

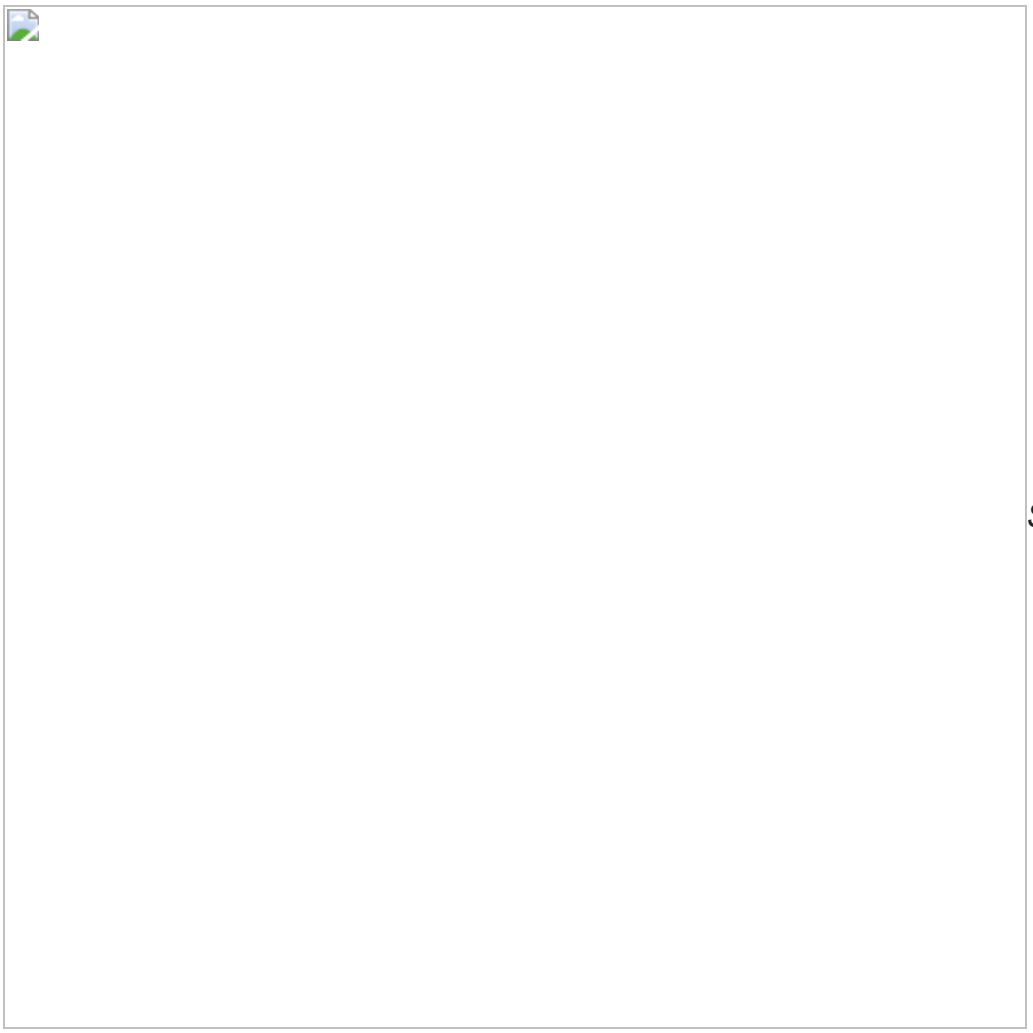
Flashpoint analysts have identified a post on the Russian language XSS Forum in which a threat actor operating under the alias of “Ekranoplan” posted a possible master key for REvil in a screenshot on Github.[1] Thus far, Flashpoint analysts have been able to attribute this

key to restoration of data associated with the recent Kaseya ransomware attack, and are exploring whether there is broader applicability.

REvil (aka, “Sodinokibi” or “Sodin”) is a Russian ransomware extortionist threat group that is responsible for several high-visibility ransomware incidents in recent months, including the attack against technology provider Kaseya. While REvil was purportedly shut down in July 2021, many of their targets remain impacted by their activities, and other groups have recently emerged that Flashpoint analysts assess as being related to REvil.

Ekranoplan shared a link to the screenshot on August 6, 2021. The user does not appear to have any further posting history on the forum. Several users questioned the utility of a screenshot in decrypting files, to which Ekranoplan answered in Russian, “This was provided to us by our parent company and is supposed to work for all REvil victims, not just us.” While the origins of Ekranoplan are unknown, no pun intended, Flashpoint analysts tested the REvil decryptor. As one user in the thread highlighted, replacing the decryption key with this key should work.

Flashpoint patched the decryptor binary with the annotated key from the thread, and successfully decrypted a sandbox infected with the new REvil test sample, upon changing the file extensions to “universal_tool_xxx_yyy” as seen in the screenshot. The files were properly decrypted once the file extensions were renamed.



Screenshot of masterkey posting from Github. Posting in XSS Forum, as seen (and translated) in the Flashpoint platform

Similar to the Russian aircraft owing to Ekranoplan's namesake, the user flew out of the forum thread as quickly as they entered. The mystery still remains on the true reason for REvil's sudden disappearance. Whether their infrastructure was the target of a coordinated law enforcement operation, the decryption key was leaked by a former victim, or a change of heart from the REvil operators remains a point of conjecture. At this time, the outcome is the same. Analysts will continue to monitor for changes in the ransomware ecosystem.

Track Ransomware Activity With Flashpoint

The data above was discovered directly through analyst research in the Flashpoint platform. Sign up for a free trial, and see firsthand how Flashpoint can help you and your organization access the most critical information affecting your industry and the security community.

Sources: [1] hxxps://github[.]com/Fr3akaLmaTT3r/decryptor/blob/main/screenshot.png