

REvil ransomware hits Managed.com hosting provider, 500K ransom

By Lawrence Abrams

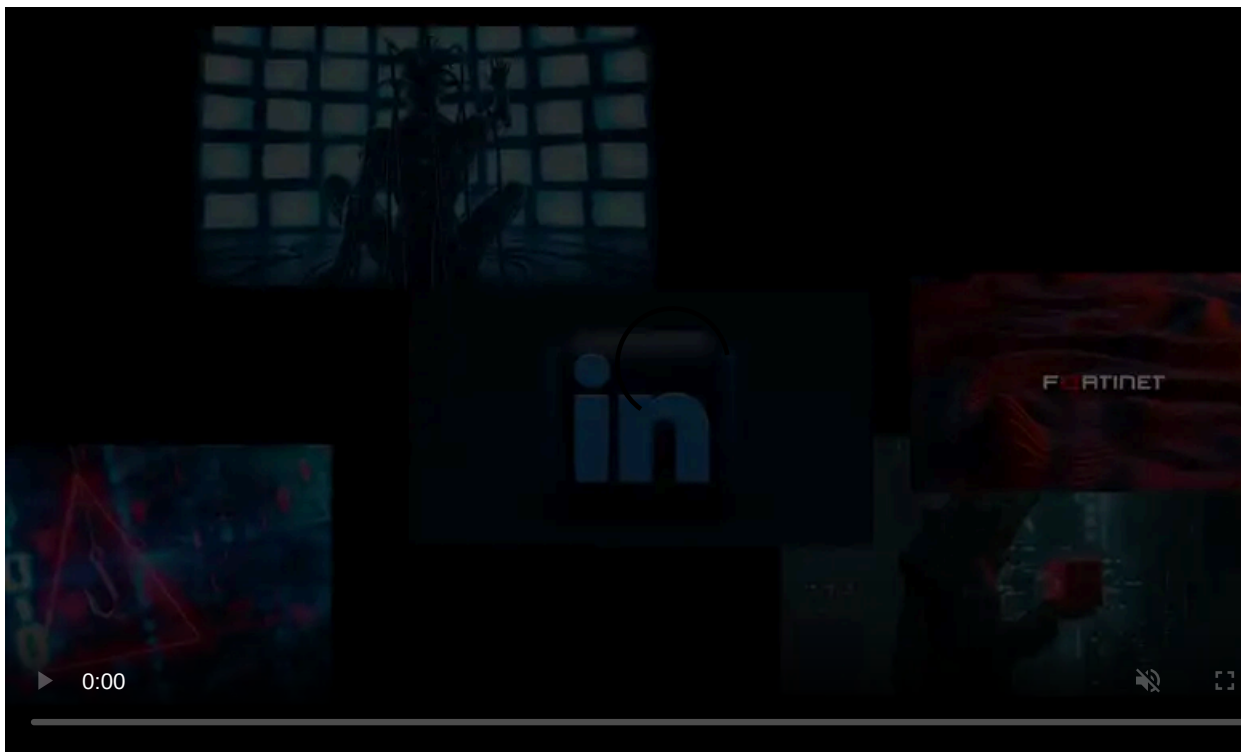
Published: 2020-11-18 · Archived: 2026-04-05 20:16:06 UTC



Managed web hosting provider Managed.com has taken their servers and web hosting systems offline as they struggle to recover from a weekend REvil ransomware attack.

On Monday morning, Managed.com announced that they had suffered an issue affecting the availability of their hosting services and are investigating the matter.

As first reported by [ZDNet](#), Managed.com disclosed on Tuesday that they were hit with a ransomware attack and, to protect the "integrity of our customer's data," they decided to take their entire system down, including clients' websites.



Visit Advertiser website [GO TO PAGE](#)

"November 17, 2020 – On Nov.16, the Managed.com environment was attacked by a coordinated ransomware campaign. To ensure the integrity of our customers' data, the limited number of impacted sites were immediately taken offline. Upon further investigation and out of an abundance of caution, we took down our entire system to ensure further customer sites were not compromised. Our Technology and Information Security teams are working diligently to eliminate the threat and restore our customers to full capacity. Our first priority is the safety and security of your data. We are working directly with law enforcement agencies to identify the entities involved in this attack. As more information is available, we will communicate directly with you," Managed.com stated in a [status update](#).

At the time of this writing, websites for Managed.com hosting clients continue to be unavailable, leading to some clients [switching their web hosting](#) to another provider.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at [+16469613731](#) or on Wire at [@lawrenceabrams-bc](#).

REvil demanding a \$500 thousand ransom

Since learning of the attack, multiple sources have told BleepingComputer that Managed.com was hit by the ransomware operation known as REvil.

According to a screenshot shared with BleepingComputer, REvil is demanding a \$500,000 ransom in Monero to receive a decryptor. It is not known if the ransomware operation stole unencrypted files before encrypting devices.

The screenshot shows a ransomware payment interface. At the top, it says "General-Decryptor price" and "the price is for all PCs of your infected network". Below this, there is a countdown timer: "You have 5 days, 12:40:45". To the right, the "Current price" is listed as "4072.655 XMR" which is approximately "≈ 500,000 USD". Below the current price, it says "After time ends" and the price will increase to "8145.31 XMR" or "≈ 1,000,000 USD". There are two asterisked notes: "* If you do not pay on time, the price will be doubled" and "* Time ends on Nov 24, 07:02:59". At the bottom left, there is a "Monero address:" followed by a long alphanumeric string. At the bottom right, a note states "* XMR will be recalculated in 1 hour with an actual rate."

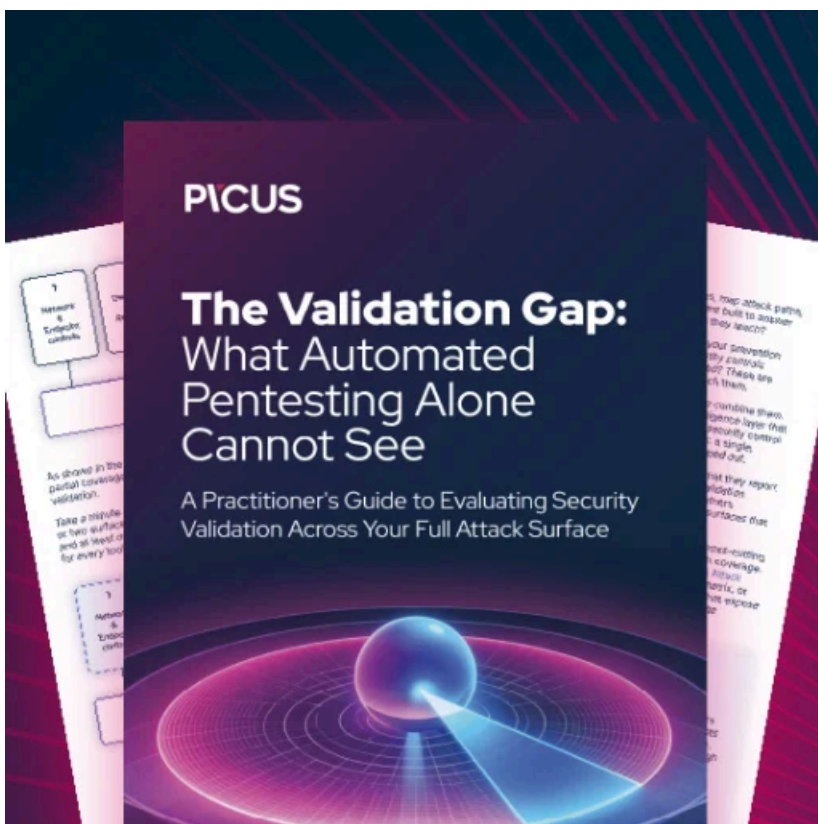
Ransom amount for Managed.com

REvil is a Ransomware-as-a-Service that [began infecting victims](#) in April 2019 and has since grown to become one of the largest ransomware operations currently operating.

In a recent interview with the public-facing representative of REvil, the ransomware operation claims to [earn over \\$100 million a year](#) in extortion payments.

REvil has been responsible for large attacks in the past, including [Travellex](#), [Kenneth Cole](#), [SeaChange](#), [Brown-Forman](#), and celebrity law firm [Grubman Shire Meiselas & Sacks](#) (GSMLaw).

BleepingComputer has contacted Managed.com with questions related to the attack but has not heard back.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/>