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

bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/

Lawrence Abrams

By
Lawrence Abrams

- November 18, 2020
- 10:53 AM
- 0

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.

"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.

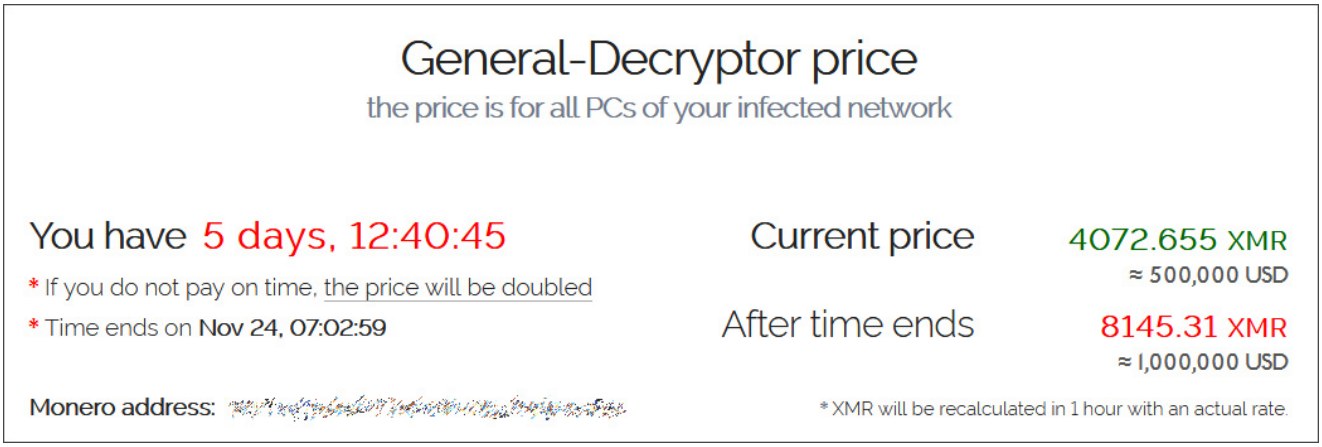
At the time of this writing, websites for Managed.com hosting clients continue to be unavailable, leading to some clients switching their web hosting to another provider.

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.



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 Travelex, 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.

Related Articles:

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

REvil ransomware returns: New malware sample confirms gang is back

REvil's TOR sites come alive to redirect to new ransomware operation

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.