TA505 Hackers Behind Maastricht University Ransomware Attack

bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/

Sergiu Gatlan

By
Sergiu Gatlan

- February 7, 2020
- 04:45 PM
- 3

Maastricht University (UM) disclosed that it paid the 30 bitcoin ransom requested by the attackers who encrypted some of its critical systems following a cyberattack that took place on December 23, 2019.

UM is a university from the Netherlands with roughly 4,500 employees, 18,000 students, and 70,000 alumni, placed in the top 500 universities in the world by five different ranking tables during the last two years.

"Part of our technical infrastructure was affected during the attack. That infrastructure consists of 1,647 Linux and Windows servers and 7,307 workstations," the university explains in a management summary of the Fox-IT incident report and UM's response.

"The attack ultimately focused on 267 servers of the Windows domain. The attacker focused on encrypting data files in the Windows domain. The backup of a limited number of systems was also affected."

UM says that all critical systems now have online and offline backups to avoid facing a future total failure scenario in the event of another ransomware attack.

Fox-IT connects TA505 to the attack

"The modus operandi of the group behind this specific attack comes over with a criminal group that already has one has a long history, and goes back to at least 2014," says Fox-IT in its full report to UM (in Dutch).

TA505 (also tracked SectorJ04) is a financially motivated hacker group known for mainly targeting retail companies and financial institutions since at least Q3 2014. (1, 2)

They are also known for using remote access Trojans (RATs) and malware downloaders that delivered the Dridex and Trick banking Trojans as secondary payloads during their campaigns, as well as several ransomware strains including Locky, BitPaymer, Philadelphia, GlobeImposter, and Jaff on their targets' computers[1, 2] now also including Clop ransomware after the attack on UM.

According to Fox-IT, the hackers were able to infiltrate the university's systems via two phishing e-mails that were opened on two UM systems on October 15 and 16.

Until November 21 when they gained admin rights on an unpatched machine, the attackers moved through UM's network compromising servers left and right until it finally deployed the Clop ransomware payload on 267 Windows systems.

The university paid the ransom to have the files decrypted on December 30 after closely analyzing the options including rebuilding all infected systems from scratch or attempting to create a decryptor.

"During the investigation, traces were found that show that the attacker collected data regarding the topology of the network, usernames, and passwords of multiple accounts, and other network architecture information," the report summary says.

Also, Fox-IT says that it "did not find any traces within the scope of the investigation that point to the collection of other types of data."

Ransom paid to avoid data loss and months of downtime

After the attack, UM secured the services of security company Fox-IT to assist with the incident's forensic investigation, the crisis management process, and to provide advice during the recovery according to official statements part of a press conference from February 5.

While UM added that the forensic research "indicates how cybercriminals have taken some of UM's data hostage," research and personal data was not exfiltrated.

However, the university will continue investigating if this conclusion is 100% accurate via "follow-up research into possible extraction" of important data files representative of education, research, and business operations as Fox-IT recommends.

UM also disclosed that it acquired the ransomware decryptor from the attackers by paying a 30 bitcoin ransom (roughly $220,000 or €220,000) to restore all the encrypted files as Reuters reported.

This allowed UM to avoid having to rebuild all the compromised systems from scratch, losing all the research, educational, and staff data and delaying exams and salary payments to the university's 4,500 employees.

"It is a decision that was not taken lightly by the Executive Board. But it was also a decision that had to be made," UM says. "We felt, in consultation with our management and our supervisory bodies, that we could not make any other responsible choice when considering the interests of our students and staff.

"The fact that on 6 January and thereafter we were able to have teaching and exams take place, more or less as planned, that UM researchers suffered little or no irreparable damage, and that we were also able to make the salary payments for 4,500 employees on time, strengthens our confidence that we made the right choice."

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

Austin Peay State University resumes after ransomware cyber attack

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

- Cyberattack
- Netherlands
- Ransomware
- TA505
- University

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Comments

- 
  JettLoftus - 2 years ago
  -
  -
  it`s very terrible hackers attack for university!
- 
  JamesWillmott - 2 years ago
  -
  -
  just horror
- 
  QuidProQuo - 1 year ago
  -
  -
  Free vacation for the students!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: