Home › News › Security › Ransomware Attacks Hit Everis and Spain's Largest Radio Network

Ransomware Attacks Hit Everis and Spain's Largest Radio Network

By **Sergiu Gatlan**

November 4, 2019 12:56 PM **0**

Everis, an NTT DATA company and one of Spain's largest managed service providers (MSP), had its computer systems encrypted today in a ransomware attack, just as it happened to Spain's largest radio station Cadena SER (Sociedad Española de Radiodifusión).

While the ransomware attacks were not yet publicly acknowledged by the company, the ransom note left on Everis' encrypted computers has already leaked and BleepingComputer can confirm that the MSP's data was infected using the BitPaymer ransomware.

BitPaymer used in MSP attack

After the attack began, Everis sent an internal notification saying that they "are suffering a massive virus attack on the Everis network. Please keep the PCs off."

"The network has been disconnected with clients and between offices. We will keep you updated. Please, send urgently the message directly to your teams and colleagues due to standard communication problems," Everis added.

> *Esta parece ser la nota que everis ha mandado a sus trabajadores. #ransomware pic.twitter.com/1UOT8jDO4s*
>
> *— Arnau Estebanell Castellví (@ArnauEstebanell) November 4, 2019*

The ransomware encrypted files on the company's systems using the .3v3r1s extension, further exposing the targeted nature of this attack against the MSP.

The ransom note that got planted on Everis' encrypted systems warns the company against disclosing the incident while also providing it with contact details "to get the ransom amount." The email contacts listed in the ransom note are sydney.wiley@protonmail.com and evangelina.mathews@tutanota.com, but these change per targeted attack.

The attackers asked Everis for a €750,000 ($835,923) ransom to get a decryption key to unlock their files as reported by bitcoin.es.

Everis ransom note (*Alex Barredo*)

Unknown ransomware encrypts radio's systems

Everis was not alone in getting hit by a ransomware attack today as Cadena SER, the largest radio station network in Spain, was also hit by an unknown ransomware.

"The SER chain has suffered this morning an attack of computer virus of the ransomware type, file encrypter, which has had a serious and widespread affectation of all its computer systems," Cadena SER says in a notification published today.

Following the attack that used an unknown ransomware strain, the radio station had to disconnect all of its computers from the Internet and it is currently continuing activity with the help of equipment at its Madrid headquarters.

"The technicians are already working for the progressive recovery of the local programming of each of their stations," Cadena SER adds.

Spain's Department of Homeland Security (Departamento de Seguridad Nacional) also confirmed the ransomware attack that impacted Cadena SER as did Spain's INCIBE (Instituto Nacional de Ciberseguridad).

INCIBE is currently helping the radio station to restore their encrypted data and get their systems back online.

Possible MSP downstream attacks

A tactic more commonly being used by ransomware attackers is to target MSPs and use their management software to push the ransomware down to the MSPs' clients.

While it is not known if these are unrelated cyberattacks, cybersecurity consultant Arnau Estebanell Castellví implied that Everis may have been the source. According to a tweet by Castellví, Orange cut off Everis' access to the network in order to prevent the ransomware attack from affecting them.

> *Trabajadores de @orange_es me confirman que ellos tampoco han sido afectados por el ataque. Lo único que se ha hecho es cortar acceso a @everis y se estan tomando medidas preventivas. De momento las cosas funcionan con normalidad.*
>
> *— Arnau Estebanell Castellví (@ArnauEstebanell) November 4, 2019*

BleepingComputer has not been able to independently corroborate this statement.

BlueKeep potentially exploited in the attacks

BleepingComputer has learned from a source close to one of the attacks who wishes to remain anonymous that the BlueKeep vulnerability is reportedly involved in these attacks.

Furthermore, in light of the BlueKeep mass exploitation discovered over the weekend, some say [1, 2] that this vulnerability was leveraged in today's ransomware attacks against Spanish organizations but there is no clear evidence to support this theory.

The BlueKeep exploitation attempts have been recorded by security expert Kevin Beaumont's honeypots that expose only the 3389 port used for remote assistance connections via the Remote Desktop Protocol (RDP).

Beaumont also found today that Everis has hundreds of servers directly exposed to Internet connections, something that hints at the possibility of the rumors of BlueKeep exploitation in today's ransomware attacks being true.

> *Oh boy, these guys appear to have hundreds of RDP servers directly on the internet HT @binaryedgeio data pic.twitter.com/d7wGjP4J6S*
>
> *— Kevin Beaumont (@GossiTheDog) November 4, 2019*

Castellví told BleepingComputer that, while "nothing is confirmed right now", Everis' internal network being down could be explained through exploiting BlueKeep or the other two RDP vulnerabilities patched some time ago.

"I think the initial vector might be email. That is what the Spanish National Security Center has said," he added. "But after patient 0, I also think it is RDP-based. If not, there is no explanation of why the internal network of Everis is down."

Whether BlueKeep was actually involved is not yet clear at this point.

Bleeping Computer asked CERT Spain, Everis, and SER for more details but did not hear back at the time of publication.

Update November 04, 13:07 EST: Added comments from cybersecurity consultant Arnau Estebanell Castellví.

Related Articles:

TrialWorks Ransomware Attack Disrupts Court Cases and Deadlines

Office 365 Adds Malware ZAP Toggle to Security & Compliance Center

Billing Provider Billtrust Suffers Outage After Malware Attack

Global Shipping Firm Pitney Bowes Affected by Ransomware Attack

Apple Software Update Zero-Day Used by BitPaymer Ransomware

BITPAYMER BLUEKEEP MALWARE MSP RADIO RANSOMWARE SPAIN

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

Post a Comment

Community Rules

You need to login in order to post a comment

Login

Not a member yet? Register Now

You may also like:

Hackers Ask for $5.3 Million Ransom, Turn Down $400k,…

bleepingcomputer.com

Author of Original Petya Ransomware Publishes Master…

bleepingcompute

Maze Ransomware Says Computer Type Determines…

bleepingcomputer.com

Android Trojan Infects Tens of Thousands of…

bleepingcomputer.com

How to Pro
Harden a C
against Ra

bleepingcompute

POPULAR STORIES

Malwarebytes 4.0 Released With New UI and Scanning Engine

BEC Fraudsters Divert $742,000 from Ocala City in Florida