Nokia subsidiary discloses data breach after Conti ransomware attack

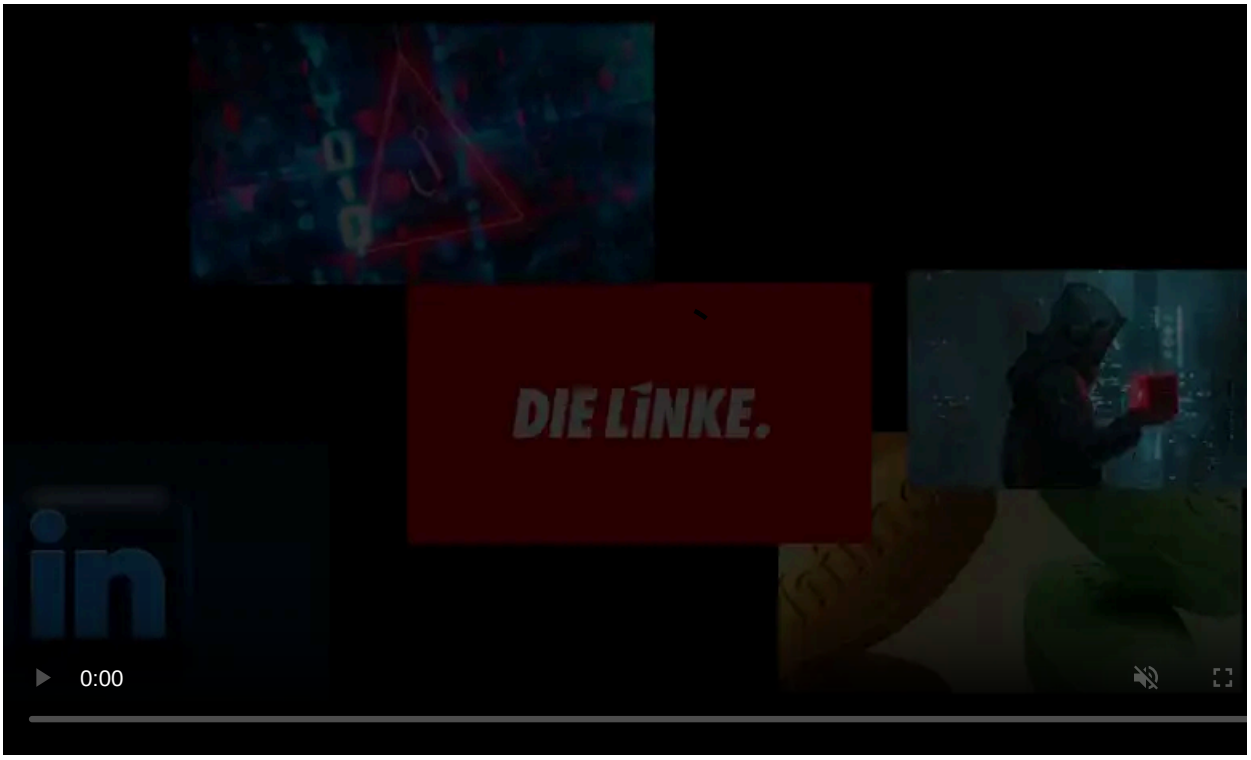
By Sergiu Gatlan

Published: 2021-08-23 · Archived: 2026-04-05 13:08:04 UTC

Image: Kabiur Rahman Riyad

SAC Wireless, a US-based Nokia subsidiary, has disclosed a data breach following a ransomware attack where Conti operators were able to successfully breach its network, steal data, and encrypt systems.

The wholly-owned and independently-operating Nokia company, headquartered in Chicago, IL, works with telecom carriers, major tower owners, and original equipment manufacturers (OEMs) across the US.


DIE LINKE.
0:00

Attack detected after Conti ransomware encrypted systems

The company discovered that its network was breached by Conti ransomware operators on June 16, only after deploying their payloads and encrypting SAC Wireless systems.

The Nokia subsidiary found that personal information belonging to current and former employees (and their health plans' dependents
or beneficiaries) was also stolen during the ransomware attack on August 13, following a forensic investigation conducted with the help of external cyber security experts.

"The threat actor, Conti, gained access to the SAC systems, uploaded files to its cloud storage, and then, on June 16, deployed ransomware to encrypt the files on SAC systems," SAC says in data breach notification letters sent to an undisclosed number of impacted individuals.

After completing the forensic investigation, the company believes that the stolen files contain the following categories of personal info: "name, date of birth, contact information (such as home address, email, and phone), government ID numbers (such as driver's license, passport, or military ID), social security number, citizenship status, work information (such as title, salary, and evaluations), medical history, health insurance policy information, license plate numbers, digital signatures, certificates of marriage or birth, tax return information, and dependent/beneficiary names."

In response to the ransomware attack, SAC has taken multiple measures to prevent future breaches, including:

- changed firewall rules,
- disconnected VPN connections,
- activated conditional access geo-location policies to limit non-U.S. access,
- provided additional employee training,
- deployed additional network and endpoint monitoring tools,
- expanded multi-factor authentication,
- and deployed additional threat-hunting and endpoint detection and response tools.

BleepingComputer reached out to SAC Wireless for additional information on the attack two weeks ago, on August 12, but a company spokesperson refused to confirm that it involved ransomware or provide additional details.

"SAC is aware of an incident, and we are currently investigating the matter," the spokesperson said. "As we continue to assess the incident, we are in contact with relevant parties to recommend that appropriate safeguards and precautions may be taken."

Conti claims to have stolen 250GB of files

While the company refused to acknowledge the ransomware attack and did not provide more info on the extent of the damage, the Conti ransomware gang revealed on their leak site that they stole over 250 GB of data.

According to a recent update, the ransomware group will soon leak all the stolen files online if the Nokia subsidiary doesn't pay the ransom they demanded.

Conti ransomware is a private Ransomware-as-a-Service (RaaS) operation likely controlled by a Russian-based cybercrime group known as Wizard Spider.

Conti shares some of its code with the notorious Ryuk Ransomware, whose TrickBot distribution channels they began using after Ryuk decreased activity around July 2020.

The gang has recently breached Ireland's Health Service Executive (HSE) and Department of Health (DoH), asking the former to pay a $20 million ransom after encrypting its systems.

The FBI also warned in May that Conti operators have attempted to breach the networks of more than a dozen US healthcare and first responder organizations.

Earlier this month, a disgruntled affiliate leaked the gang's training materials, including information about one of its operators, a manual on deploying Cobalt Strike and mimikatz, as well as numerous help documents allegedly provided to affiliates when performing Conti attacks.

Source: https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-conti-ransomware-attack/