Migration policy org confirms cyberattack after extortion group touts theft

By Jonathan Greig

Published: 2023-01-11 · Archived: 2026-04-06 03:11:16 UTC

The International Centre for Migration Policy Development (ICMPD) confirmed on Wednesday it suffered a cyberattack that led to a data breach.

ICMPD operates in 90 countries conducting research, projects and activities centered around migration. It currently has 19 member states — most of which are European — and has observer status at the United Nations. It works with several UN and European agencies as well as states across Africa, Asia and South America.

Bernhard Schragl, communication coordinator for ICMPD, did not say when the attack took place but told The Record that the attackers managed to gain "limited access" to individual servers that held data.

ICMPD set up a task force of internal and external IT experts who are currently investigating the incident.

"Professional preparation as well as quick and decisive actions have prevented the attackers from inflicting additional harm. In less than 45 minutes after detection, an emergency response team was established, all external network connections were disconnected and all websites taken down to prevent the attack from spreading further," Schragl said.

The organization is in the process of investigating what information was compromised, according to Schragl, who added that they have reported the incident to law enforcement agencies.

Schragl said ICMPD has either already informed or plans to inform any who had data that was affected by the attack about measures that need to be taken to protect themselves.

The attack on ICMPD was launched by the Karakurt extortion group, which boasted on Telegram of stealing financial documents, banking data and personal information.

On its leak site, the hacking group further explained that it stole 375 GB of data that included "correspondence on contracts, scans of contracts, project budgets, financial and insurance documents, invoices, passports, mailboxes of key members of the organization and much more."

In June, the FBI, Cybersecurity and Infrastructure Security Agency (CISA), and the Treasury Department released an alert about Karakurt, warning that the group was holding victim data for ransoms of $25,000 to $13 million in Bitcoin.

"Karakurt actors have typically provided screenshots or copies of stolen file directories as proof of stolen data. Karakurt actors have contacted victims' employees, business partners, and clients with harassing emails and phone calls to pressure the victims to cooperate," the alert explained.

"As of May 2022, the website contained several terabytes of data purported to belong to victims across North America and Europe, along with several 'press releases' naming victims who had not paid or cooperated, and instructions for participating in victim data 'auctions,'" CISA added.

The agencies noted that Karakurt does not target specific industries or companies, often choosing victims based on ease of access.

The group typically gains access to systems by either purchasing stolen login credentials or purchasing access to victims who have been compromised by other cybercriminals.

> With our partners @FBI, @USTreasury and FinCEN, @CISAgov issued a joint cybersecurity advisory on #Karakurt data extortion group. Known ransom demands ranged from $25K to $13M in Bitcoin. Mitigate your risk: https://t.co/gNiDbLsNJQ pic.twitter.com/0ft8mPediO
>
> — Jen Easterly (@CISAJen) June 1, 2022

Emsisoft threat analyst Brett Callow previously told The Record that the group has been active since the middle of 2021 and is believed to be a spin-off of the Conti ransomware group.

Several other security companies — including Infinitum IT and Advanced Intelligence — have released reports this year showing concrete ties between the infrastructure used by Conti and Karakurt.

Following the release of troves of documents and chats related to Conti, security companies found numerous links between the two groups.

Advanced Intelligence said Karakurt is a side business of the group behind Conti, allowing them to monetize the data stolen during attacks where organizations are able to block the ransomware encryption process.

Blockchain analysis firm Chainalysis has also previously identified several cryptocurrency wallets controlled by Karakurt which sent funds to Conti.

The U.S. agencies confirmed much of what was reported by these security companies, highlighting that Karakurt has attacked victims in the midst of ransomware incidents.

In several cases seen by CISA and the FBI, victims have gotten ransom notes from multiple ransomware variants simultaneously, "suggesting Karakurt actors purchased access to a compromised system that was also sold to another ransomware actor."

The attack on ICMPD comes just a few months after hackers targeted the Red Cross. In January, the international aid organization said it had been hacked in November by a group that stole data from a program called Restoring Family Links, a web-based system used by Red Cross volunteers to reunite family members separated by conflict, disaster, or migration.

The attack was so alarming to governments around the world that the U.S. State Department released a statement calling the attack a "dangerous development" that had "real consequences.

“This cyber incident has harmed the global humanitarian network’s ability to locate missing people and reconnect families,” officials said.

“This is why it is so vital that humanitarian data be respected and only used for intended purposes.”

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
