Kia Motors America suffers ransomware attack, $20 million ransom

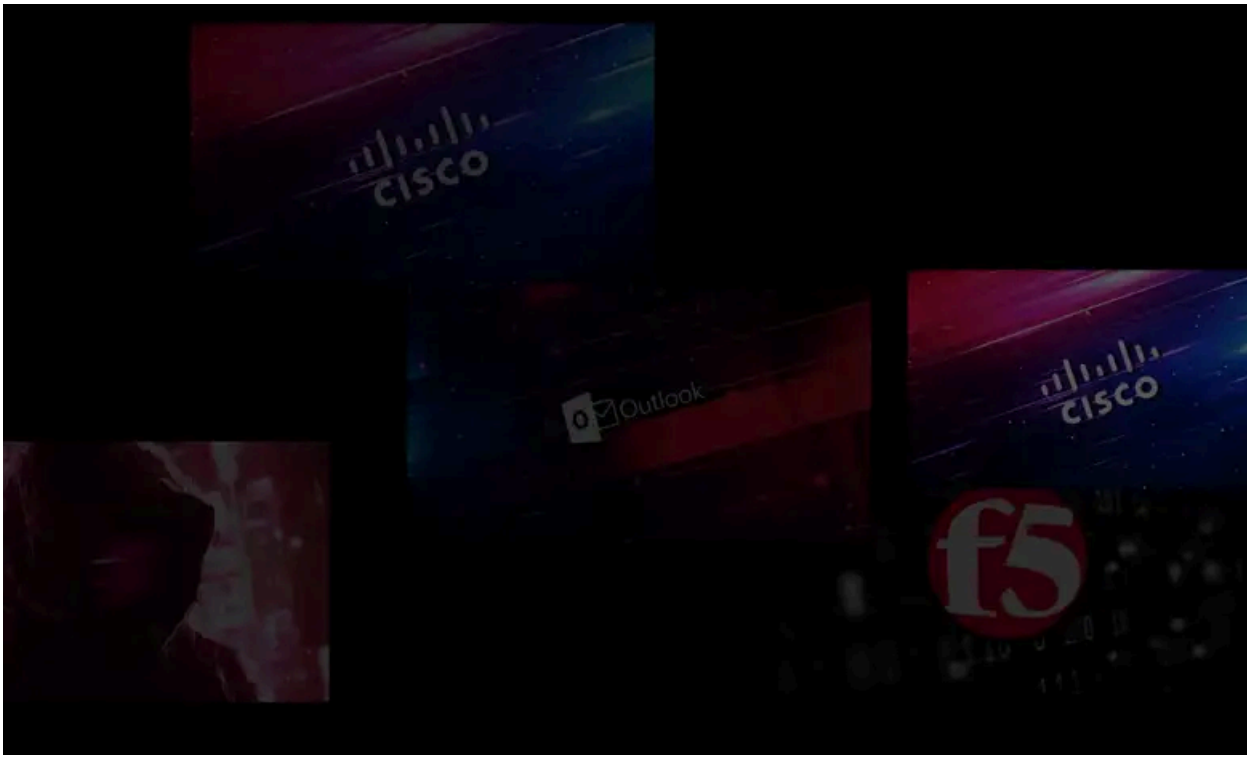
By Lawrence Abrams

Published: 2021-02-17 · Archived: 2026-04-02 12:14:05 UTC

Story updated with Kia Motors America statement below.

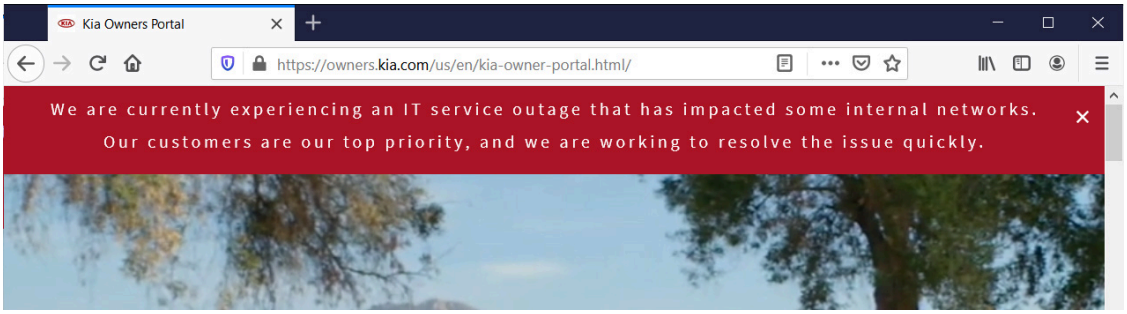
Kia Motors America has suffered a ransomware attack by the DoppelPaymer gang, demanding $20 million for a decryptor and not to leak stolen data.

Kia Motors America (KMA) is headquartered in Irvine, California, and is a Kia Motors Corporation subsidiary. KMA has nearly 800 dealers in the USA with cars and SUVs manufactured out of West Point, Georgia.


cisco
Outlook
cisco
f5

Yesterday, we reported that Kia Motors America was suffering a nationwide IT outage that has affected their mobile UVO Link apps, phone services, payment systems, owner's portal, and internal sites used by dealerships.

When visiting their sites, users are met with a message stating that Kia is "experiencing an IT service outage that has impacted some internal networks," as shown below.



A Kia owner tweeted that when they attempted to pick up their new car, a dealership told them that the servers were down due to a ransomware attack.

> @Kia I went to the Kia dealership in Arizona and signed a new lease, yet the manager told me your computers have been down for 3 days due to Ransomware and has affected Kia all over the USA. Can't get my car for ???? Now what?
>
> — Amybean (@amylee62) February 16, 2021

When we contacted Kia Motors America yesterday about these outages and ransomware reports, KMA told us that they were working on resolving the outage.

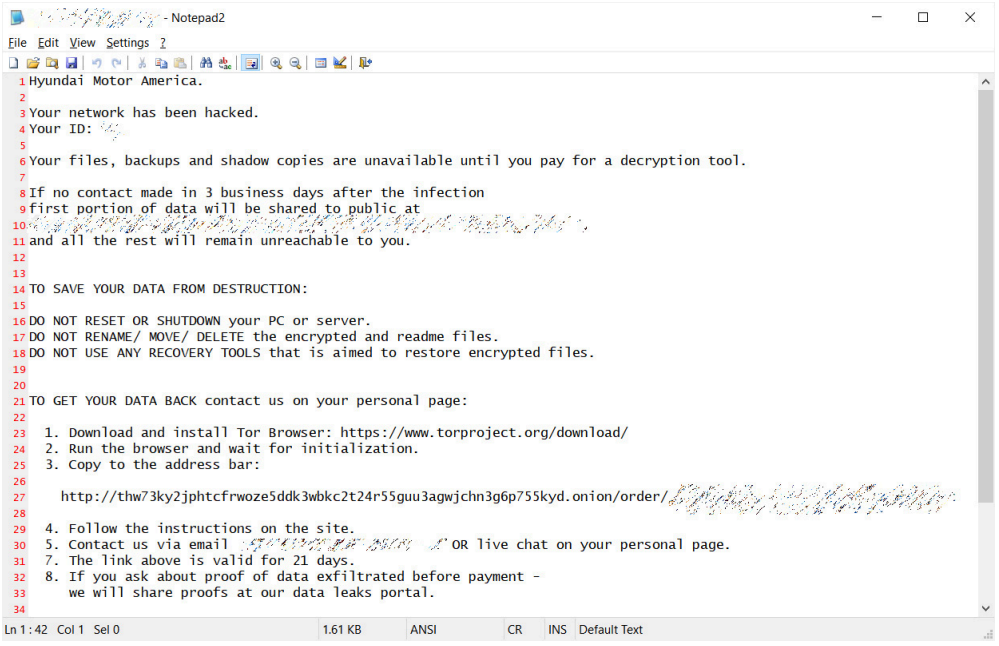
> "KMA is aware of IT outages involving internal, dealer and customer-facing systems, including UVO. We apologize for any inconvenience to our customers and are working to resolve the issue and restore normal business operations as quickly as possible." - Kia Motors America.

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.

Kia was attacked by the DoppelPaymer ransomware

Today, BleepingComputer obtained a ransom note that we were told was created during an alleged Kia Motors America cyberattack by the DoppelPaymer ransomware gang.

In a ransom note seen by BleepingComputer, the attackers state that they attacked Hyundai Motor America, Kia's parent company. Hyundai does not appear to be affected by this attack.



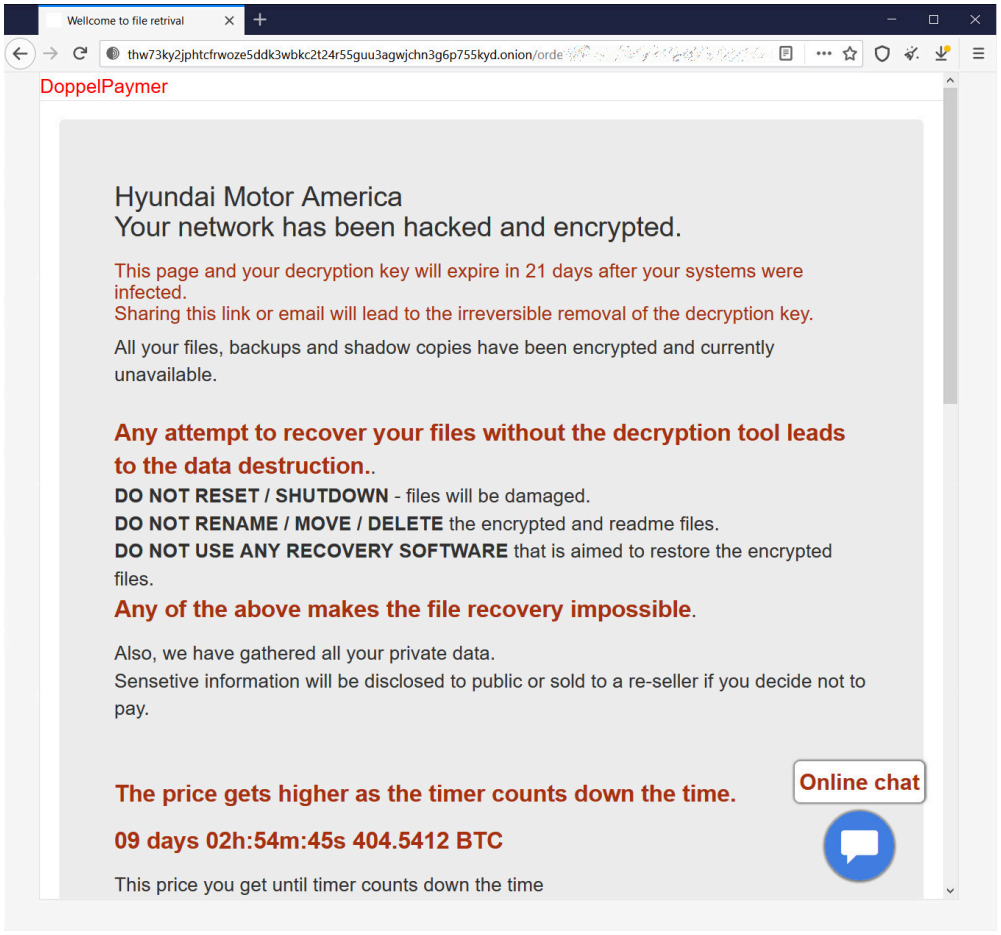
Kia Motors America ransom note

Source: BleepingComputer

The ransom note contains a link to a private victim page on the DoppelPaymer Tor payment site that once again states the target is 'Hyundai Motor America.'

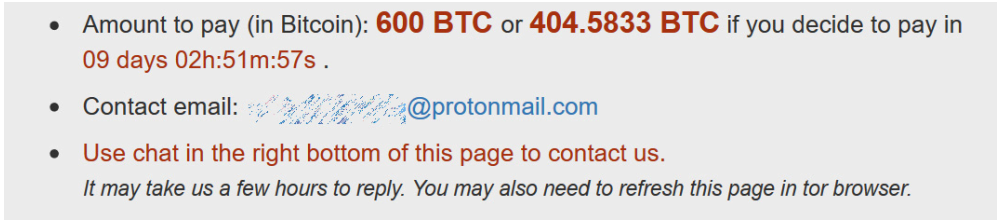
The Tor victim page says that a "huge amount" of data was stolen, or exfiltrated, from Kia Motors America and that it will be released in 2-3 weeks if the company does not negotiate with the threat actors.

DoppelPaymer is known for stealing unencrypted files before encrypting devices and then posting portions on their data leak site to further pressure victims into paying.



Tor payment page for the Kia ransomware attack
Source: BleepingComputer

To prevent the leak of the data and receive a decryptor, DoppelPaymer is demanding 404 bitcoins worth approximately $20 million. If a ransom is not paid within a specific time frame, the amount increases to 600 bitcoins, or $30 million.



404 bitcoin ransom demand
Source: BleepingComputer

The DoppelPaymer operation has not indicated what type of data has been stolen. Based on the amount of Kia services suffering an outage, we can expect a wide range of affected servers.

The stealing of unencrypted files has become a widely used tactic by ransomware operations to coerce victims to pay, with Emsisoft stating it has affected more than 1,300 companies globally.

"Globally, more than 1,300 companies, many US-based, lost data including intellectual property and other sensitive information. Note, this is simply the number of companies which had data published on leak sites and takes no account of the companies which paid to prevent publication," states Emsisoft's 2020 State of Ransomware report.

Other well-known victims attacked by DoppelPaymer in the past include Foxconn, Compal, PEMEX (Petróleos Mexicanos), the City of Torrance in California, Newcastle University, Hall County in Georgia, Banijay Group SAS, and Bretagne Télécom.

Update 2/17/21: In a statement to BleepingComputer, Kia Motors America has stated that they have seen no evidence that they have suffered a "ransomware" attack.

Kia Motors America, Inc. (“Kia”) is currently experiencing an extended systems outage. Affected systems include the Kia Owners Portal, UVO Mobile Apps, and the Consumer Affairs Web portal. We apologize for any inconvenience to affected customers, and are working to resolve the issue as quickly as possible with minimal interruption to our business. We are also aware of online speculation that Kia is subject to a “ransomware” attack. At this time, we can confirm that we have no evidence that Kia or any Kia data is subject to a “ransomware” attack.

We have once again reached out and asked if they were impacted by a "cyberattack" but have not heard back.

Hyundai also experienced outages

After the publishing of this story, numerous Hyundai and dealership employees contacted BleepingComputer to state that Hyundai was also affected by unexplained outages.

In emails sent by Hyundai Motors America to Kia dealerships on Saturday and seen by BleepingComputer, Hyundai stated that multiple systems were down including their internal dealer site, hyundaidealer.com.

BleepingComputer was also told that services used by dealer technicians were affected as well.

Since then, some of these services have since been restored.

In a similarly worded statement as Kia, Hyundai told BleepingComputer that they have no evidence of a "ransomware" attack.

> "At this time, we can confirm that we have no evidence of Hyundai Motor America’s involvement in a “ransomware” attack." - Hyundai Motors America

BleepingComputer reached out to confirm if they were impacted by a cyberattack but has not heard back.

This is a developing story.

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
