Novel Meteor Wiper Used in Attack that Crippled Iranian Train System

By Elizabeth Montalbano

Published: 2021-07-30 · Archived: 2026-04-10 03:11:44 UTC

A July 9th attack disrupted service and taunted Iran's leadership with hacked screens directing customers to call the phone of Iranian Supreme Leader Khamenei with complaints.

An attack earlier this month on Iran's train system, which disrupted rail service and taunted Iran's leadership via hacked public transit display screens, used a never-before-seen wiper malware called Meteor that appears to have been design for reuse, a security researcher has found.

The initial attack, dubbed MeteorExpress, occurred July 9, when "a wiper attack paralyzed the Iranian train system," according to a report by Juan Andres Guerrero-Saade at SentinelOne.

That attack disrupted service and directed customers via all of the displays and message boards at the train station to call "64411"–the number for the office of Supreme Leader Ali Khamenei—for more information.

The next day, attackers also hit the website and computer systems of the staff of Iran's the Ministry of Roads and Urban Development, according to a published report.

SentinelLabs researchers reconstructed most of the attack chain in the train-system and discovered the novel wiper, which the threat actors—who also appear to be a new set of adversaries still finding their attack rhythm–refer to as Meteor, Guerrero-Saade wrote.

Guerrero-Saade credited security researcher Anton Cherepanov with identifying an early analysis of the event written in Farsi by an Iranian antivirus company as helping researchers recreate the attack.

What they discovered is that "behind this outlandish tale of stopped trains and glib trolls" are "the fingerprints of an unfamiliar attacker," using a wiper that "was developed in the past three years and was designed for reuse," Guerrero-Saade wrote.

Reconstructing the Attack

Overall, the toolkit that orchestrated the attack was comprised of a combination of batch files that implemented different components dropped from RAR archives, according to SentinelLabs. Attackers used the batch files, nested alongside their respective components, in a chain to successfully execute the attack.

“The wiper components are split by functionality: Meteor encrypts the filesystem based on an encrypted configuration, nti.exe corrupts the MBR, and mssetup.exe locks the system,” Guerrero-Saade wrote.

Researchers recovered “a surprising amount of files” for a wiper attack, but did not manage to reconstruct them all. One missing notable component was the MBR corrupter, nti.exe; its absence is significant because files overwritten by this component are the same as those overwritten by the notorious NotPetya ransomware, which crippled organizations around the world in 2017, Guerrero-Saade noted.

Despite the attack’s success, however, researchers found “a strange level of fragmentation to the overall toolkit,” he said.

“Batch files spawn other batch files, different RARarchives contain intermingled executables, and even the intended action is separated into three payloads: Meteor wipes the filesystem, mssetup.exe locks the user out, and nti.exe presumably corrupts the MBR,” Guerrero-Saade wrote.

Specific Attack Components

Researchers identified and elaborated two of those three payloads in the report. One is the main payload, the Meteor wiper, which comes in the form of an executable dropped under env.exe or msapp.exe,and is executed as a scheduled task with a single argument–an encrypted JSON configuration file, msconf.conf, that holds values for corresponding keys contained in cleartext within the binary, according to the report.

“At its most basic functionality, the Meteor wiper takes a set of paths from the encrypted config and walks these paths, wiping files,” Guerrero-Saade wrote. “It also makes sure to delete shadow copies and removes the machine from the domain to avoid means of quick remediation.”

The wiper also includes much more functionality that was not used in the Iranian train attack, he noted. It can: change passwords for all users; disable screensavers; terminate processes based on a list of target processes; install a screenlocker; disable recovery mode; changesboot policy error handling; create scheduled tasks; and log off local sessions, among other actions.

The fact that it has such broad capabilities seems to suggest that Meteor is not merely a one-off, but that its creators intend for it to be used in other attacks, Guerrero-Saade noted.

MeteorExpress attackers also dropped a standalone screenlocker, mssetup.exe,that blocks user input before creating a window that fills the entire screen before disabling the cursor and locking the user out entirely, according to the report.

Novice Attackers?

Despite its success in the MeteorExpress attack, the threat group seems still to be honing their skills and finding their way, as evidenced by the “contradictory” practices of Meteor’s code and capabilities, researchers observed.

“First, the code is rife with sanity checks, error checking, and redundancy in accomplishing its goals,” Guerrero-Saade wrote. “However, the operators clearly made a major mistake in compiling a binary with a wealth of debug strings meant for internal testing.”

The guts of Meteor also include a “bizarre amalgam of custom code” that leverages open-source components and “practically ancient” software–FSProLabs’ Lock My PC 4, pointing to the general experimental nature of the attackers’ approach, he said.

However, “while that might suggest that the Meteor wiper was built to be disposable, or meant for a single operation,” this code is “juxtaposed with an externally configurable design that allows efficient reuse for different operations,” Guerrero-Saade wrote.

Overall, the components of MeteorExpress that researchers examined point to a new, intermediate-level player in the attack landscape “whose different operational components sharply oscillate from clunky and rudimentary to slick and well-developed,” he concluded.

080321 14:17 UPDATE: Corrected name of SentinelOne.

Source: https://threatpost.com/novel-meteor-wiper-used-in-attack-that-crippled-iranian-train-system/168262/