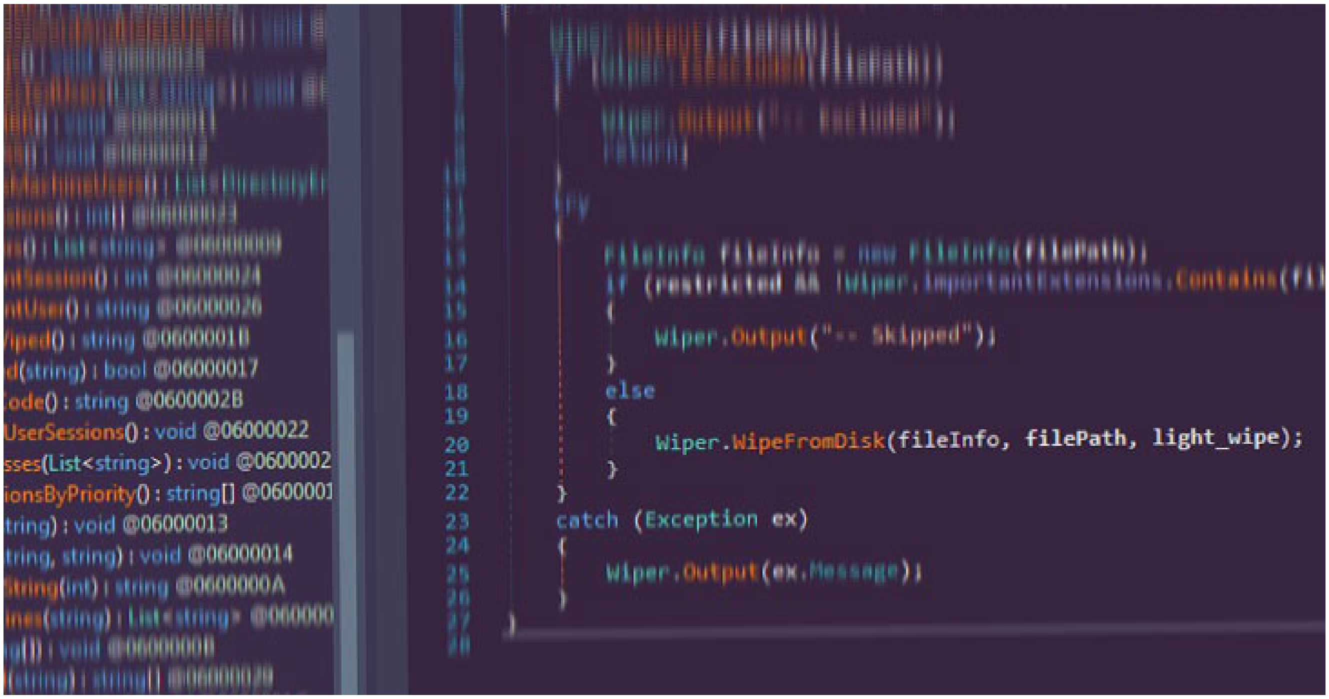
Iranian State Broadcaster IRIB Hit by Destructive Wiper Malware

thehackernews.com/2022/02/iranian-state-broadcaster-irib-hits-by_21.html

February 21, 2022

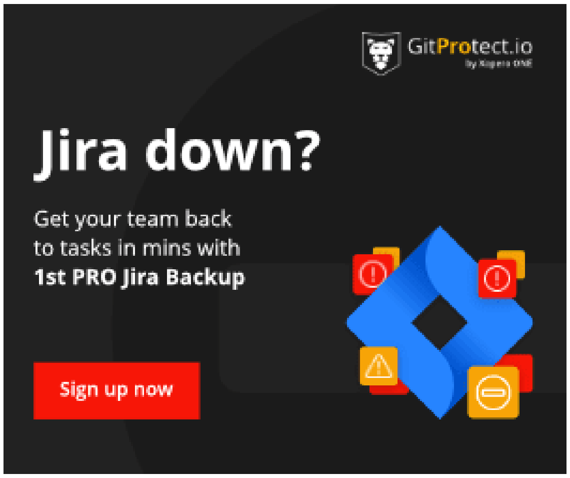


```
        Wiper.Output("-- Excluded");
        return;
    }
    try
    {
        FileInfo fileInfo = new FileInfo(filePath);
        if (restricted && !Wiper.ImportantExtensions.Contains(fi
        {
            Wiper.Output("-- Skipped");
        }
        else
        {
            Wiper.WipeFromDisk(fileInfo, filePath, light_wipe);
        }
    }
    catch (Exception ex)
    {
        Wiper.Output(ex.Message);
    }
}
```

An investigation into the cyberattack targeting Iranian national media corporation, Islamic Republic of Iran Broadcasting (IRIB), in late January 2022 revealed the deployment of a wiper malware and other custom implants, as the country's national infrastructure continues to face a wave of attacks aimed at inflicting serious damage.

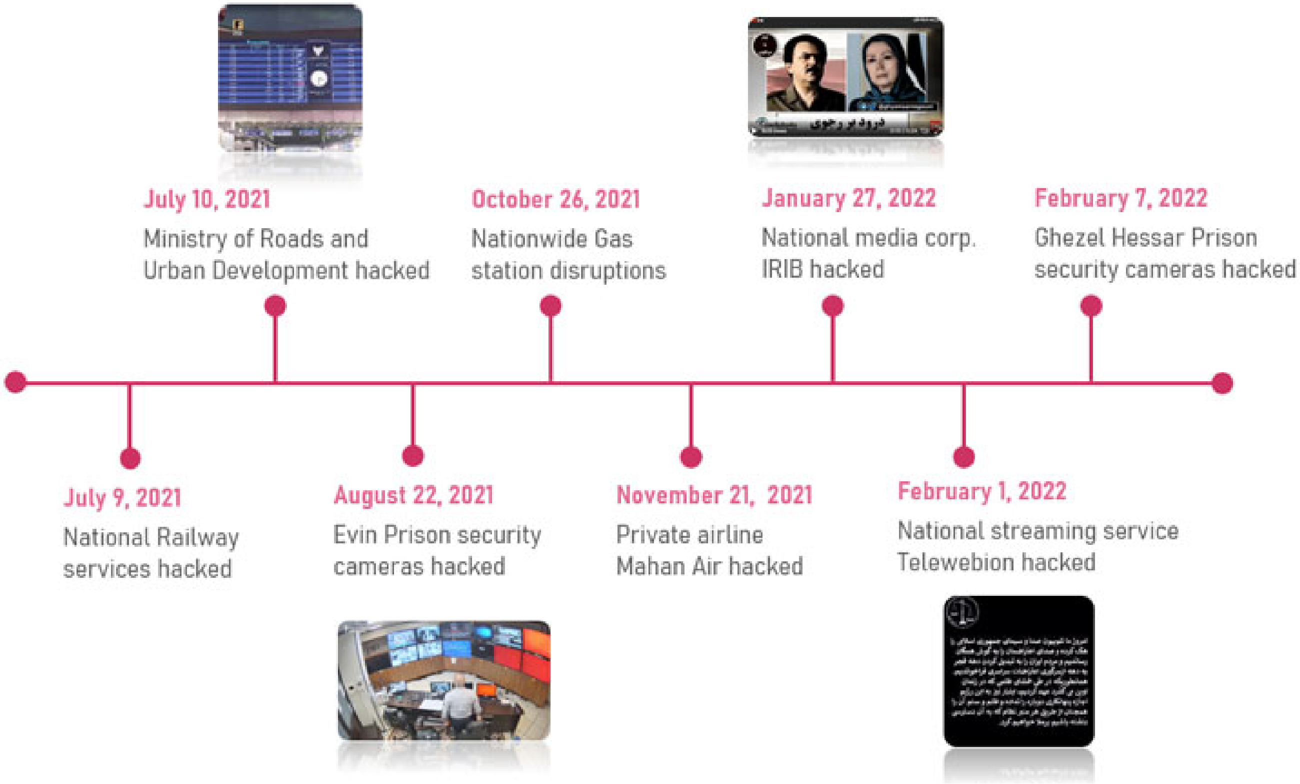
"This indicates that the attackers' aim was also to disrupt the state's broadcasting networks, with the damage to the TV and radio networks possibly more serious than officially reported," Tel Aviv-based cybersecurity firm Check Point said in a report published last week.

The 10-second attack, which took place on January 27, involved the breach of state broadcaster IRIB to air pictures of Mujahedin-e-Khalq Organization (MKO) leaders Maryam and Massoud Rajavi alongside a call for the assassination of the Supreme Leader Ayatollah Ali Khamenei.



"This is an extremely complex attack and only the owners of this technology could exploit and damage the backdoors and features that are installed on the systems," Deputy IRIB chief Ali Dadi was quoted as saying to state TV channel IRINN.

Also deployed during the course of the hack were custom-made malware capable of taking screenshots of the victims' screens as well as backdoors, batch scripts, and configuration files used to install and configure the malicious executables.


July 10, 2021
Ministry of Roads and Urban Development hacked
October 26, 2021
Nationwide Gas station disruptions
January 27, 2022
National media corp. IRIB hacked
February 7, 2022
Ghezel Hessar Prison security cameras hacked
July 9, 2021
National Railway services hacked
August 22, 2021
Evin Prison security cameras hacked
November 21, 2021
Private airline Mahan Air hacked
February 1, 2022
National streaming service Telewebion hacked

Check Point said it didn't have enough evidence to make a formal attribution to a specific threat actor, and it's currently not known how the attackers gained initial access to the targeted networks. Artifacts uncovered so far include files responsible for –

- Establishing backdoors and their persistence,
- Launching the "malicious" video and audio files, and
- Installing the wiper malware in an attempt to disrupt operations in the hacked networks.

Behind the scenes, the attack involved interrupting the video stream using a batch script to delete the executable associated with TFI Arista Playout Server, a broadcasting software used by IRIB, and play the video file ("TSE_90E11.mp4") in a loop.

The intrusion also paved the way for the installation of a wiper whose main purpose is to corrupt the files stored in the computer, not to mention erase the master boot record (MBR), clear Windows Event Logs, delete backups, kill processes, and change users' passwords.

Furthermore, the threat actor leveraged four backdoors in the attack: WinScreeny, HttpCallbackService, HttpService and ServerLaunch, a dropper launched with HttpService. Taken together, the different pieces of malware enabled the adversary to capture screenshots, receive commands from a remote server, and carry out other malicious activities.

"On one hand, the attackers managed to pull off a complicated operation to bypass security systems and network segmentation, penetrate the broadcaster's networks, produce and run the malicious tools that heavily rely on internal knowledge of the broadcasting software used by victims, all while staying under the radar during the reconnaissance and initial intrusion stages," the researchers said.

"On the other hand, the attackers' tools are of relatively low quality and sophistication, and are launched by clumsy and sometimes buggy 3-line batch scripts. This might support the theory that the attackers might have had help from inside the IRIB, or indicate a yet unknown collaboration between different groups with different skills."

SHARE □ □ □ □ ךָ
SHARE □