TA2541: APT Has Been Shooting RATs at Aviation for Years

By Elizabeth Montalbano

Published: 2022-02-15 · Archived: 2026-04-05 16:27:17 UTC

Since 2017, the attacker has flung simple off-the-shelf malware in malicious email campaigns aimed at aviation, aerospace, transportation and defense.

Researchers have identified an advanced persistent threat (APT) group responsible for a series of cyberespionage and spyware attacks against the aviation, aerospace, transportation and defense industries since at least 2017 that feature high-volume email campaigns using industry-specific lures.

The group, which researchers have dubbed TA2541, typically sends hundreds of thousands of malicious messages – nearly always in English – that ultimately deliver a remote-access trojan (RAT) payload using commodity malware to collect data from victims' machines and networks, according to a new report by Proofpoint released Tuesday. These campaigns have affected hundreds of organizations across the world, with recurring targets in North America, Europe and the Middle East, researchers said.

Though a number of the group's attacks already have been tracked by various researchers – including Microsoft, Mandiant, Cisco Talos, Morphisec and others – since at least 2019, Proofpoint's latest research shares "comprehensive details linking public and private data under one threat activity cluster we call TA2541," researchers wrote.

Indeed, previously reported attacks related to TA2541 include a two-year spyware campaign against the aviation industry using the AsyncRAT called Operation Layover and uncovered by Cisco Talos last September, and a cyberespionage campaign against aviation targets spreading RevengeRAT or AsyncRAT revealed by Microsoft last May, among others.

Five Years and Still Flying High

Proofpoint first started tracking the actor in 2017 when its tactic of choice was to send messages with "macro-laden Microsoft Word attachments" that downloaded RAT payloads. The group has since tweaked this tactic and now most frequently sends messages with links to cloud services such as Google Drive or OneDrive hosting the payload, according to the report.

However, although the approach to how they hide their malicious payload has varied, the group has mostly remained consistent in its choice of targets, lures and the type of payloads it uses, observed Sherrod DeGrippo, vice president of Threat Research & Detection at Proofpoint.

“What’s noteworthy about TA2541 is how little they’ve changed their approach to cybercrime over the past five years, repeatedly using the same themes, often related to aviation, aerospace, and transportation, to distribute remote access trojans,” she said in an email to Threatpost. “This group is a persistent threat to targets throughout the transportation, logistics, and travel industries.”

In terms of which specific RATs are used, attackers tap a variety of low-hanging fruit – that is, commodity malware that’s available for purchase on criminal forums or available in open-source repositories. Currently, TA2541 prefers to drop AsyncRAT on victims’ machines but also is known to use NetWire, WSH RAT and Parallax, researchers said.

So far, all of the malware distributed by the group has been aimed at information-gathering purposes and to gain remote control of an infected machine, with researchers acknowledging that they don’t know the threat actor’s “ultimate goals and objectives” beyond this initial compromise, they said.

Typical Malicious Emails

A typical malicious message in a TA2541 campaign uses a lure related to some type of logistical or transportation theme related to one of the particular industries it’s targeting, researchers said.

“In nearly all observed campaigns, TA2541 uses lure themes that include transportation-related terms such as flight, aircraft, fuel, yacht, charter, etc.,” according to the report.

For example, researchers revealed an email that impersonated an aviation company requesting information on aircraft parts, as well as another that requested info on how to transport a medical patient on a stretcher on an ambulatory flight.

Once the COVID-19 pandemic hit in March 2020, the group shifted bait tactics slightly and – like many other threat actors – adopted COVID-related lures consistent with their overall theme of cargo and flight details, researchers noted.

“For example, they distributed lures associated with cargo shipments of personal protective equipment (PPE) or COVID-19 testing kits,” researchers noted.

However, this shift was short-lived, and TA2541 rather quickly returned to its more generic, transportation-related email themes, they added.

Current Attack Vector

In current campaigns observed by Proofpoint, if victims take the bait, they will usually be directed to click on a Google Drive URL that leads to an obfuscated Visual Basic Script (VBS) file, researchers said.

“If executed, PowerShell pulls an executable from a text file hosted on various platforms such as Pastetext, Sharetext, and GitHub,” researchers wrote. “The threat actor executes PowerShell into various Windows processes and queries Windows Management Instrumentation (WMI) for security products such as antivirus and firewall software, and attempts to disable built-in security protections.”

In this way, TA2541 collects system information before then downloading the RAT on the host machine, according to the report.

Google Drive has been a consistent tool of the threat group, but occasionally TA2541 also will use OneDrive to host the malicious VBS files, researchers said. In late 2021, Proofpoint also observed the group using DiscordApp URLs that link to a compressed file that led to either AgentTesla or Imminent Monitor as an attack vector, researchers said. Indeed, the Discord content delivery network (CDN) has been an increasingly popular way for threat actors to use a legitimate and popular app for nefarious purposes.

Occasionally TA2541 also will use email attachments instead of cloud-based service links, including compressed executables such as RAR attachments with an embedded executable containing URL to CDNs hosting the malware payload, they added.

Join Threatpost on Wed. Feb 23 at 2 PM ET for a LIVE roundtable discussion "The Secret to Keeping Secrets," sponsored by Keeper Security, focused on how to locate and lock down your organization's most sensitive data. Zane Bond with Keeper Security will join Threatpost's Becky Bracken to offer concrete steps to protect your organization's critical information in the cloud, in transit and in storage. REGISTER NOW and please Tweet us your questions ahead of time @Threatpost so they can be included in the discussion.

Source: https://threatpost.com/ta2541-apt-rats-aviation/178422/