Unskilled hacker linked to years of attacks on aviation, transport sectors

bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/

Ionut Ilascu

By
Ionut Ilascu

- February 15, 2022
- 07:28 AM
- 1

For years, a low-skilled attacker has been using off-the-shelf malware in malicious campaigns aimed at companies in the aviation sector as well as in other sensitive industries.

The threat actor has been active since at least 2017, targeting entities in the aviation, aerospace, transportation, manufacturing, and defense industries.

Tracked as TA2541 by cybersecurity company Proofpoint, the adversary is believed to operate from Nigeria and its activity has been documented before in analysis of separate campaigns.

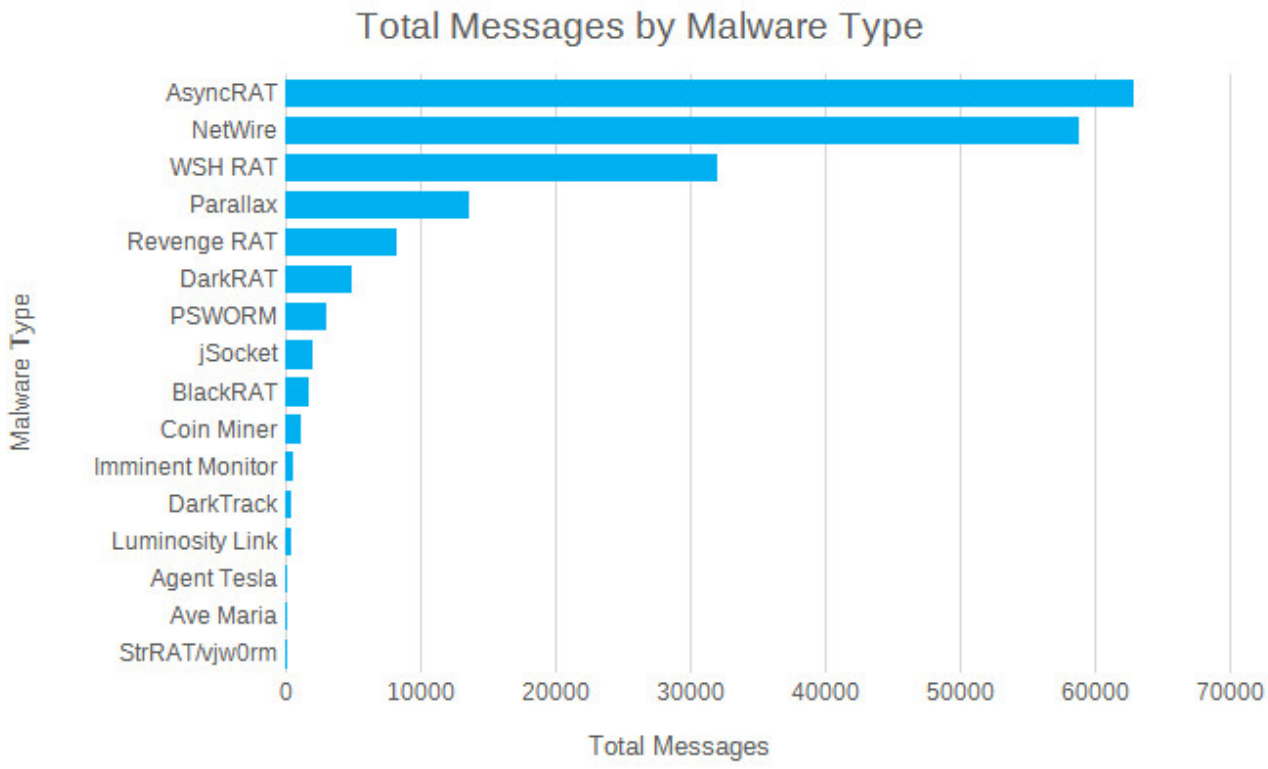
Non-sophisticated attacks

In a report today, Proofpoint notes that TA2541 has been consistent about its attack method, relying on malicious Microsoft Word documents to deliver a remote access tool (RAT).

A typical malware campaign from this group involves sending “hundreds to thousands” of emails - mostly in English - to “hundreds of organizations globally, with recurring targets in North America, Europe, and the Middle East.”

Recently, though, the group switched from malicious attachments to linking to a payload hosted in cloud services such as Google Drive, Proofpoint researchers say.

TA2541 does not use custom malware but commodity malicious tools available for purchase on cybercriminal forums. According to the researcher’s observations, AsyncRAT, NetWire, WSH RAT, and Parallax appears to be the group’s top favorites being pushed most often in malicious messages.



source: Proofpoint

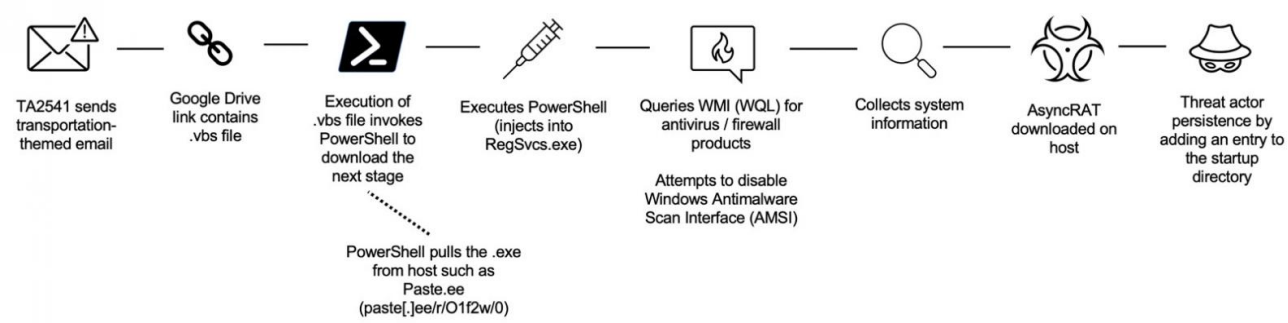
Proofpoint highlights that all malware used in TA2541 campaigns can be used to collect information, but the threat actor’s ultimate goal remains unknown at the moment.

A typical TA2541 attack chain starts with sending an email that is usually related to transportation (e.g. flight, aircraft, fuel, yacht, charter, cargo) and delivers a malicious document.

“In recent campaigns, Proofpoint observed this group using Google Drive URLs in emails that lead to an obfuscated Visual Basic Script (VBS) file. If executed, PowerShell pulls an executable from a text file hosted on various platforms such as Pastetext, Sharetext, and GitHub” - Proofpoint

In the next step, the adversary executes PowerShell into various Windows processes and looks for available security products by querying the Windows Management Instrumentation (WMI).

Then it tries to disable the built-in defenses and starts gathering system information before downloading the RAT payload on the compromised host.



source: Proofpoint

Given TA2541’s choice of targets, its activity has not gone unnoticed and security researchers from other companies have analyzed its campaigns [1, 2, 3] in the past, but without connecting all the dots.

Cisco Talos published a report last year about a TA2541 campaign targeting the aviation industry with AsyncRAT. The researchers concluded that the actor had been active for at least five years.

Based on evidence from analyzing the infrastructure used in the attack, Cisco Talos was able to build a profile for the threat actor, linking its geographic location to Nigeria.

“While researching the actor's activities, using passive DNS telemetry, we compiled the list of IPs used by the domain akconsult.linkpc.net. The chart below shows that roughly 73 percent of the IPs were based in Nigeria, further strengthening the theory that the actor in question is based in Nigeria.” - Cisco Talos

In a single campaign, the actor can send up to several thousand emails to dozens of organizations and are not tailored for individuals with specific roles. This shows that TA2541 is not concerned with the stealth of its actions, further supporting the theory of a non-skilled actor.

While thousands of organizations have been targeted in these “spray-and-pray” attacks, companies across the globe in the aviation, aerospace, transportation, manufacturing, and defense industries appear to be a constant target.

Even if TA2541's tactics, techniques, and procedures (TTPs) describe an adversary that is not technically sophisticated, the actor managed to deploy malicious campaigns for more than five years without raising too many flags.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Ukraine supporters in Germany targeted with PowerShell RAT malware

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

Hackers use modified MFA tool against Indian govt employees

- Phishing
- RAT
- Remote Access Trojan
- TA2541

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

Skyward_Ho - 3 months ago

-
-

You would think that a person with these intentions would have at some point have considered his targets and the federal protections afforded to each of them. Although much more of a chore there was some benefit to having to posses a certain amount of skill when accessing the internet of the 90's. Not that it didn't contain it's own dark holes.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: