Space Pirates Target Russian Aerospace

By PolySwarm Tech Team

Archived: 2026-04-05 13:34:13 UTC

BackgroundPositive Technologies recently reported on an espionage campaign in which a previously unknown threat actor group targeted the Russian aerospace industry. Researchers at Positive Technologies dubbed the group Space Pirates.

About The CampaignPositive Technologies first encountered the campaign in late 2019 after discovering a phishing email targeting an entity in the Russian aerospace industry. The malware payload was previously unknown. In 2020, Positive Technologies researchers again encountered the same malware while responding to an incident at a Russian government organization. During the course of the investigation, researchers discovered multiple malware families leveraging the same infrastructure. In mid-2021, the researchers encountered similar attacks at two more organizations.

The campaign targeted government agencies and IT departments, aerospace, and critical infrastructure in Russia, Georgia, and Mongolia. The threat actor also reportedly targeted multiple Chinese entities in the financial vertical.

According to Positive Technologies, the TTPs in the campaign do not clearly match any known APT group. They named the previously unknown group Space Pirates. The researchers presume the threat actors are of Chinese nexus due to the presence of the Chinese language in resources, SFX archives, and PDB paths, as well as due to TTP overlaps with previously identified Chinese threat actor groups.

Multiple tools used in the campaign included MyKLoadClient, Zupdax, Downloader.Climax.A, Downloader.Climax.B, RTLShare, PlugX, BH_A006, and Deed RAT.

MyKLoadClientMyKLoadClient was distributed via spearphishing emails. It is a loader using SFX archives combined with DLL side-loading through an auxiliary launcher library signed by McAfee Inc. The launcher gives threat actors close control over the infection.

ZupdaxZupdax backdoor is written in C++ and has been active since at least 2014. It appears to be the same as the Korplug payload. Zupdax uses the UDT protocol to interact with the C2. It collects and sends system information and allows the threat actors to interact with the victim's machine.

Downloader.Climax.A and Downloader.Climax.B In this campaign, the threat actors utilized two loaders using Russian text decoy documents. Downloader.Climax.A is associated with bamo.ocry[.]com, 45.77.244[.]191, and 45.76.145[.]22. Researchers could not determine which malware the downloader delivered. Downloader.Climax.B leverages vulnerabilities in Microsoft Equation Editor.

RTLShareThe RTLShare payload is based on the same code used in PcShare backdoor but has its own execution chain involving three separate DLLs. The initial infection stage uses rtlstat.dll, which exports a single embedding function and extracts the next stage library rtlmake.dll. In its end-stage activity, the dropper launches the extricated DLL using regsvr32.exe and then deletes itself. The rtlmake.dll injector extracts the next stage DLL and injects its code into the rdpclip.exe process. The final DLL is rtlmain.dll, which is based on the code of PcMain, the main PcShare backdoor module.

PlugXPlugX is a backdoor RAT used by both criminals and multiple state-sponsored threat actor groups. In the variant used in the Space Pirates campaign, the main payload is implemented as a DLL, as with other PlugX versions. In the Space Pirates sample, the PLUG string differed from most variants, with the value of 0xCF455089, and the size of the configuration was non-standard at 0x1924 bytes. Some instances of this variant are extracted using a dropper with the executable named *demo.exe*.

BH_A006BH_A006 has a modified Gh0st backdoor as a payload.

Deed RAT Deed RAT is a modular backdoor, previously unknown to researchers. Deed RAT's C2 is ftp.microft.dynssl[.]com, which appears to be a part of threat actor-controlled infrastructure. The payload execution scheme is similar to that of PlugX, using a legitimate EXE file signed by Trend Micro to load a malicious DLL during execution, which in turn executes the encrypted shellcode from a tmp file. The shellcode is the main module loader. The module has three sections with different access rights. The first section contains executable code and the RX rights set for its memory area. The other two sections have the RW rights.

The main backdoor loads and manages plugins that implement various functions, and its data section contains eight encrypted plugins. Each plugin performs five utility operations: initialization, getting the numeric plugin ID, getting the name of the plugin, obtaining a link to the structure in the plugin's API functions, and releasing resources. The network plugin extracts the C2 address as a URL string and selects one of the connectors available in the NetSocket plugin. Messages are compressed using the LZNT algorithm and are encrypted using a random key with a modified Salsa20 algorithm. The backdoor also allows the malware to obtain a new C2 via the HTTP protocol. The backdoor is capable of collecting information about the system, creating a separate connection for

working with plugins, removing itself, issuing empty commands, deactivating the connection, uploading shellcode for an injection stored in the registry, and updating the main shellcode on disk.

Who are Space Pirates?According to Positive Technologies, Space Pirates are a presumably Chinese nexus threat actor group active since at least 2017. Their main objectives are espionage and information theft. Their goals potentially point to state-sponsored activity, as the campaign closely aligns with intelligence collection requirements related to China's 14th Five Year Plan. The current Five Year Plan spans from 2021-to 2025 and includes a focus on deep space exploration and satellite-based communications networks.

Space Pirates use multiple tools not previously observed in the wild. Their TTPs include but are not limited to spearphishing, MyKLoadClient, BH_A006, and Deed RAT. They also use tools employed by other threat actor groups, including Zupdax backdoor, PlugX, ShadowPad, Poison Ivy, PcShare, and ReVBShell. Space Pirates network infrastructure includes a small number of IP addresses pointed to by DDNS domains. They also use third, fourth, and subsequent level domains, such as w.asd3.as.amazon-corp.wikaba[.]com. Positive Technologies researchers observed Space Pirates TTPs overlapping with multiple Chinese threat actor groups, including Winnti (APT41), Emissary Panda (APT27), TA428, Red Foxtrot, Mustang Panda, and Night Dragon.

IOCsBelow is a selection of PolySwarm's samples associated with this campaign. Contact us for additional samples.947f042bd07902100dd2f72a15c37e2397d44db4974f4aeb2af709258953636f

Don't have a PolySwarm account? Go here to sign up for a free Community plan or to subscribe. Contact us at hivemind@polyswarm.io | Check out our blog | Subscribe to our reports

---

Source: https://blog.polyswarm.io/space-pirates-target-russian-aerospace