Parallax RAT: Common Malware Payload After Hacker Forums Promotion

By Lawrence Abrams

Published: 2020-02-13 · Archived: 2026-04-02 10:45:27 UTC

A remote access Trojan named Parallax is being widely distributed through malicious spam campaigns that when installed allow attackers to gain full control over an infected system.

Since December 2019, security researcher MalwareHunterTeam has been tracking the samples of the Parallax RAT as they have been submitted through VirusTotal and other malware submissions services.

Being offered for as low as $65 a month, attackers have started to heavily use this malware to gain access to a victim's computer to steal their saved login credentials and files or to execute commands on the computer.


f5
Outlook
Outlook

The attackers can then use this stolen data to perform identity theft, gain access to online bank accounts, or further spread the RAT to other victims.

Parallax sold on hacker forums

Since early December 2019, the Parallax RAT has been sold on hacker forums where the developers are promoting the software and offering support.

In their pitch to would-be buyers, the "Parallax Team" is promoting their product as having 99% reliability and being suitable for both professionals and beginners.

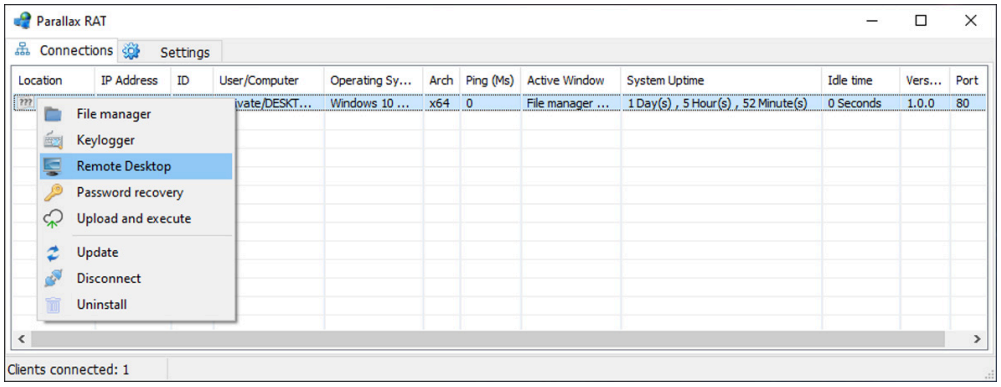
"Parallax RAT had been developed by a professional team and its fully coded in MASM.
Its created to be best in remote administration. Parallax RAT will provide you all you need.
Suitable for professionals and as well for beginners.
First and most important we offer 99% reliability when it comes to stability.
Parallax was designed to give the user a real multithreaded performance, blazing fast speed and lightweight deployment to your computers with very little resource consumption.

We are a group of developers and we are here to offer quality service.
-Parallax Team, join now!"

Attackers can purchase a one month license to the RAT for as little as $65 or $175 for a three-month license, which provides the following advertised features:

- Login credential theft
- Remote Desktop capabilities
- Upload and download files
- Execute remote commands on the infected computer
- Encrypted connections
- Supports Windows XP through Windows 10.
- Standard support

Below you can see an image of the Parallax RAT and the commands that can be executed remotely on victims.



Parallax RAT

The developers also claim that their software can bypass Windows Defender, Avast, AVG, Avira, Eset, and BitDefender, which is not true based on these detections.

Spread via malicious email attachments

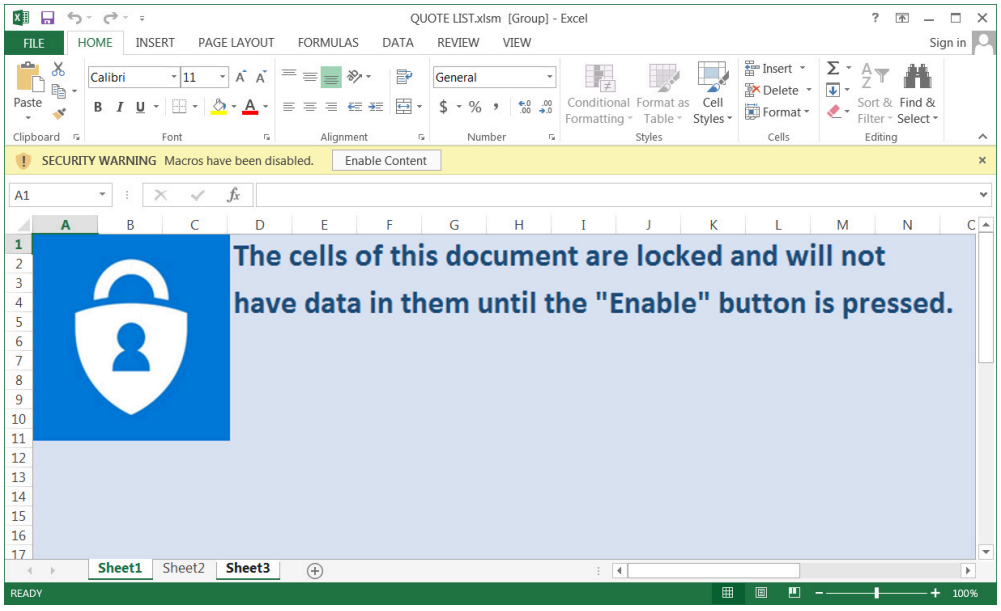
While each buyer of the Parallax RAT determines how they will distribute the malware, researchers are commonly seeing it being distributed through spam with malicious attachments.

Security research James has told BleepingComputer that it has become very common to find new spam campaigns with malicious attachments that install Parallax.

For example, the below email pretends to be a company looking to purchase products listed on an attached 'Quote List'.

Parallax Spam Campaign

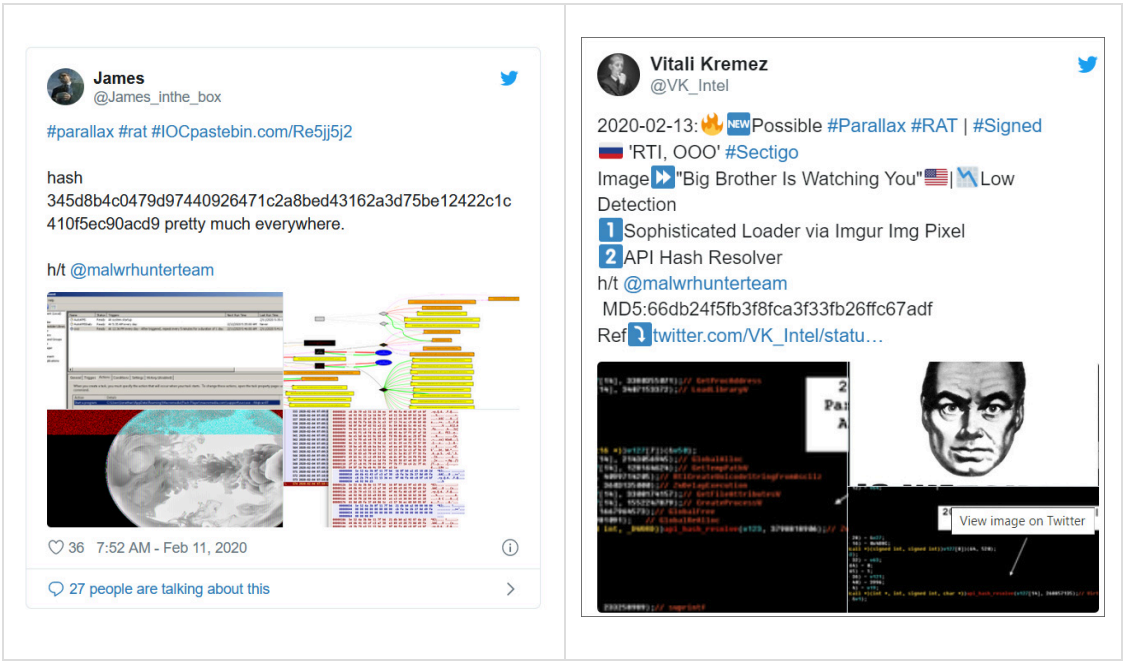
When the attachment is opened, an attempt to exploit the Microsoft Office Equation Editor vulnerability (CVE-2017-11882) will be launched and if the content is enabled, malicious macros will execute to install the RAT.



Malicious Parallax attachment

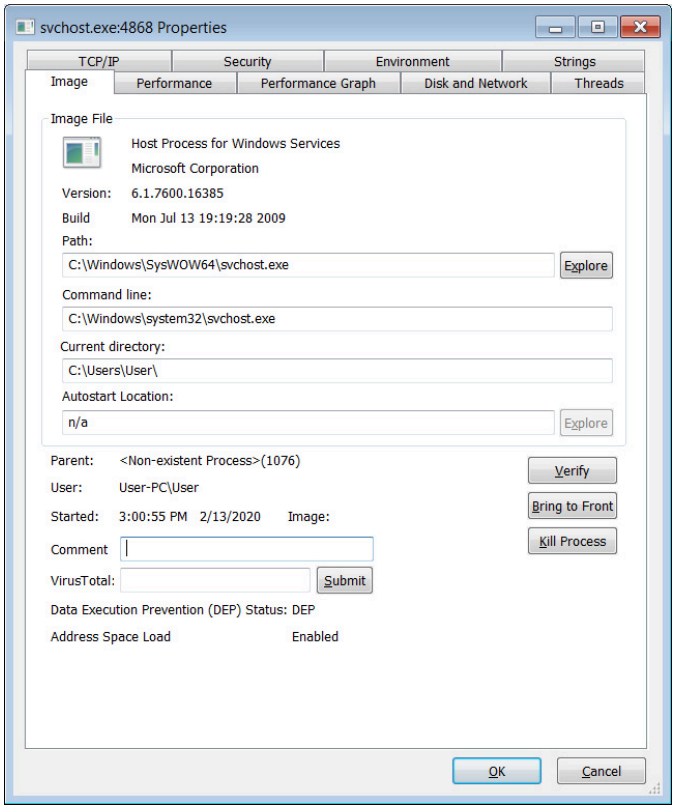
When installing the RAT, attackers are utilizing a variety of methods ranging from intermediary loaders or to directly installing the RAT onto the computer.

For example, both James and Head of SentinelLabs Vitali Kremez have seen a loader downloading an image from the Imgur image sharing site that contains an embedded Parallax executable. This executable is then extracted from the image and launched on the computer.



When executed, the RAT will either be copied to another location and executed or injected into another process.

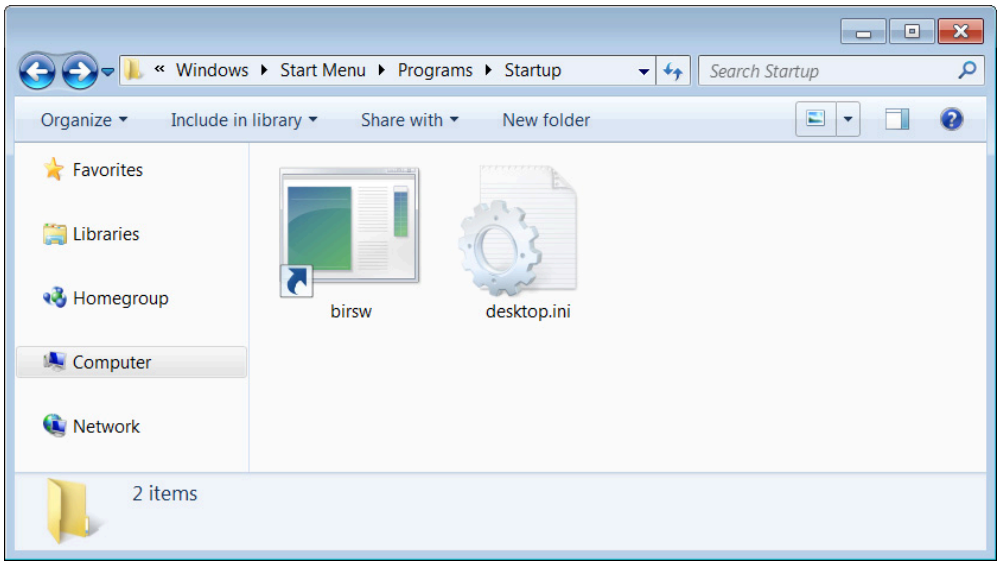
In a sample analyzed by BleepingComputer, Parallax was injected into the svchost.exe process and in another sample, Kremez saw it injected into cmd.exe.



Injected into svchost.exe

Once Parallax is installed, a shortcut to the launcher will be added to the Windows Startup folder so that it is launched automatically when a user logs into the system. In some cases, scheduled tasks will also be created to launch the malware at

various intervals.



Startup Folder

This allows the attackers to gain persistence on the infected computer and access it whenever they wish.

Now that the attackers have installed the RAT software on the computer, they can use their command and control host to steal the victim's saved passwords, steal files, execute commands, and have full control over the computer.

For many of the Parallax samples, the command & control servers are being hosted on the free dynamic DNS server duckdns.org.

As always, the best defense against this malware is to be wary of any unsolicited emails that you receive that contain attachments. Before opening them, it is best to call the sender to confirm that they sent you the email.

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
