Orcus – Birth of an unusual plugin builder RAT

By Vicky Ray

Published: 2016-08-02 · Archived: 2026-04-05 23:36:30 UTC

Unit 42 has been tracking a new Remote Access Trojan (RAT) being sold for $40 USD since April 2016, known as “Orcus”. Though Orcus has all the typical features of RAT malware, it allows users to build custom plugins and also has a modular architecture for better management and scalability. The objective of this blog is to highlight some of the capabilities of this new RAT family and the impact seen so far.

Background

Before we discuss the details of this RAT family, let's discuss how Orcus became a commercially sold RAT. Around October 2015, the developer of Orcus, going with the alias of “Sorzus”, posted a thread on a hacker forum about a RAT he was developing, soliciting feedback on how it could be published. The developer had then named the tool as “Schnorchel”, German for “Snorkel”.

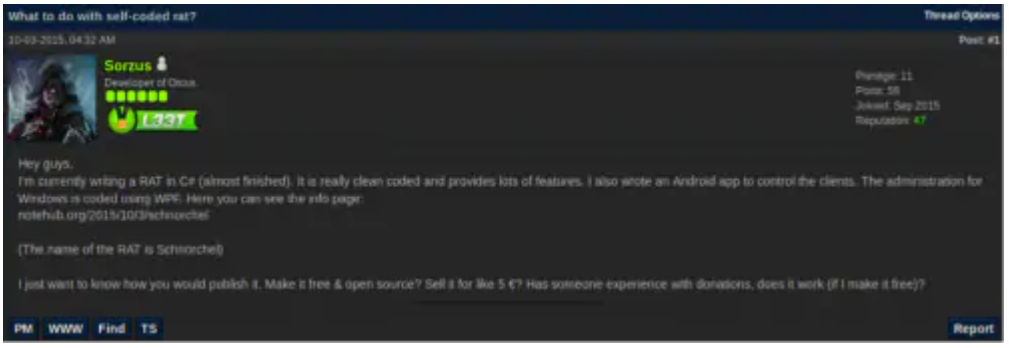

Figure 1 Sorzus discusses publishing Orcus

The figure below shows the early versions of Orcus when it was being developed. It is interesting to see that the developer details mentioned on the earlier version indicates "Vincent (Alkalinee)", and we are also aware that 'Alkalinee' was the alias which was being used by the developer before taking the new alias of 'Sorzus'. (This also suggests that the real name of the Orcus developer may be 'Vincent'.)

Figure 2 Early version of Orcus which was known as "Schnorchel"

The developer had shared intentions to publish the RAT for free and make it open-source. However, some of the users in the forum responded, advising to make it commercial instead of sharing it for free or making it open source, citing that the source code would eventually be used by others to repackage and sell it as a new RAT. One forum user, alias "Armada", offered to assist "Sorzus" on helping out with publishing the tool and apparently became Sorzus' eventual partner.

"Sorzus" and "Armada" are believed to be the two main individuals currently managing the sales and development of Orcus. Brian Krebs published a blog a few weeks ago disclosing details of the individual who has been supposedly known to be the person behind Orcus. Our analysis suggests that 'Sorzus' is the main developer of the RAT and 'Armada' is mostly responsible for sales and support of the tool.

Architecture

Orcus is developed using C# with the Windows administration/controller component developed using WPS (Windows Presentation Foundation), which is used to render user interfaces in Windows based systems. Orcus has three main components to its architecture: Orcus controller, Orcus Server and the trojan binary which is deployed on a victim machine. The delivery vectors vary, ranging from a spear phishing attack using the malware binary with the email, having a hyperlink with a download link to the Orcus malware binary, or even using drive-by download methods.

In most RAT malware, once a victim has been infected, the malware connects back to the admin panel of the attacker to send data and provide control to the infected machine. However, if a victim machine is infected with an Orcus RAT, it connects back to the Orcus server which does not have the admin panel on it. Orcus has a separate component for the admin panel (Orcus controller) which enables control of all infected machines from the Orcus controller. This set up offers multiple benefits to the cyber criminals using Orcus. For example, they are able to share access to victim machines by accessing a single Orcus server which would enable a group of cyber criminals

working together to better manage their infected victim networks and also allow scalability of their Orcus network by deploying multiple ‘Orcus servers’.

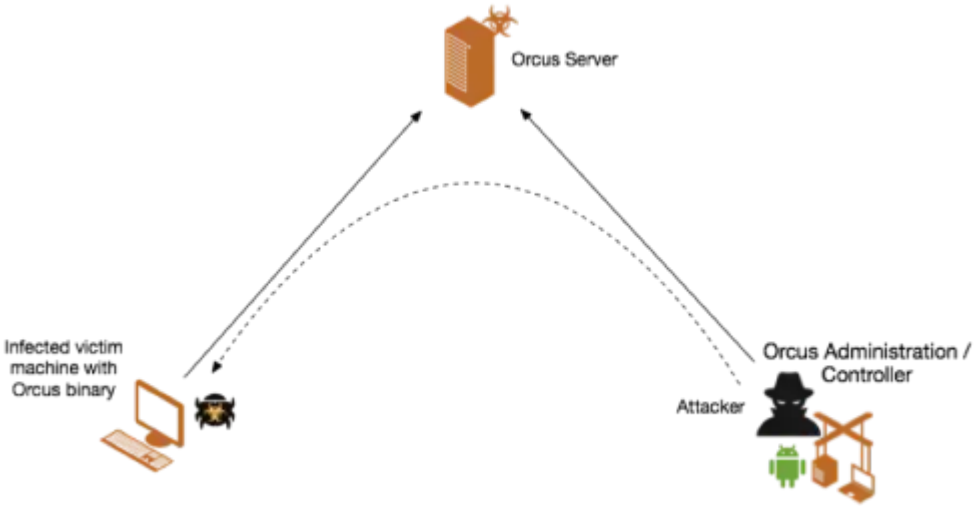

Figure 3 Orcus Architecture

The developer not only has a controller build for Windows, but also created an Android app for the admin controller to control the infected machines using an Android device. An Android app for the controller/administration component is also available from Google Play.

Figure 4 Orcus administration component for Android platform

Unique Features

Below are some Orcus features that can enable full control of a victim machine:

- Keylogger
- Screengrabs
- Remote code execution
- Webcam monitor
- Disable webcam light
- Microphone recorder
- Remote administration
- Password stealers
- Denial of Service
- VM Detection
- InfoStealer
- HVNC
- Reverse Proxy
- Registry explorer/editor
- Real Time Scripting
- Advanced Plugin System

Orcus has many common features of a RAT, however the features which are unique and stand out the most is the **‘Plugin System’** and **'Real time scripting'**. The plugin feature allows users of Orcus to build their own plugins or download plugins which have been developed by the author. If a user has basic knowledge on one of the supported programming languages, which are C#, VB.Net or C++, that user can easily extend and write plugins to build on to the current capabilities of Orcus. The author also provides a developer package to create the plugins with an IDE (Integrated Development Environment), which is an application used by programmers to develop programs.

The Orcus sellers also provide very well documented tutorials to create plugins, and also maintain a Github page which has a few sample plugins created. Orcus allows seven different types of plugins to be created. Figure 5 shows the current list of plugin types that can be built.

Type	Interface	Description	Tutorial	Example
Administration	IAdministrationPlugin	Modify the GUI of the administration window and receive serve events	Visual C#, Visual Basic	Notify Manager, Server Stress Test
Audio	IAudioPlugin	Provide audio files to play on the client's system		Audio packs
Build	IBuildPlugin	Modify the build file	Visual C#, Visual Basic	Extension Spoofer, Build Pumper
Client	ClientController	Modify the behavior of the client e. g. the startup, connection tries, installation	Visual C#, Visual Basic	BSoD protection
Command and View	Command (Client) & ICommandAndView (Administration)	Two libraries: One for the client and one for the administration. Add a new view to the client actions, can send commands to the client.	Visual C#, Visual Basic	Microphone Recorder
Factory Command and View	IFactoryClientCommand (Client) & ICommandAndView (Administration)	The same like Command and View but there's also a class which is directly loaded at startup and can collect information		Keylogger, GamerView
View	IViewPlugin	Only a view which has access to all existing commands		CLI commands

Figure 5 Types of plugins

The libraries are well documented and are currently being hosted on 'sharpdox.de'. Sharpdox is a tool to create C# code documentations and can be hosted on 'sharpdox.de'. Figure 6 shows an example of the methods or functions which are available to the Orcus plugin's 'ClientController' class.

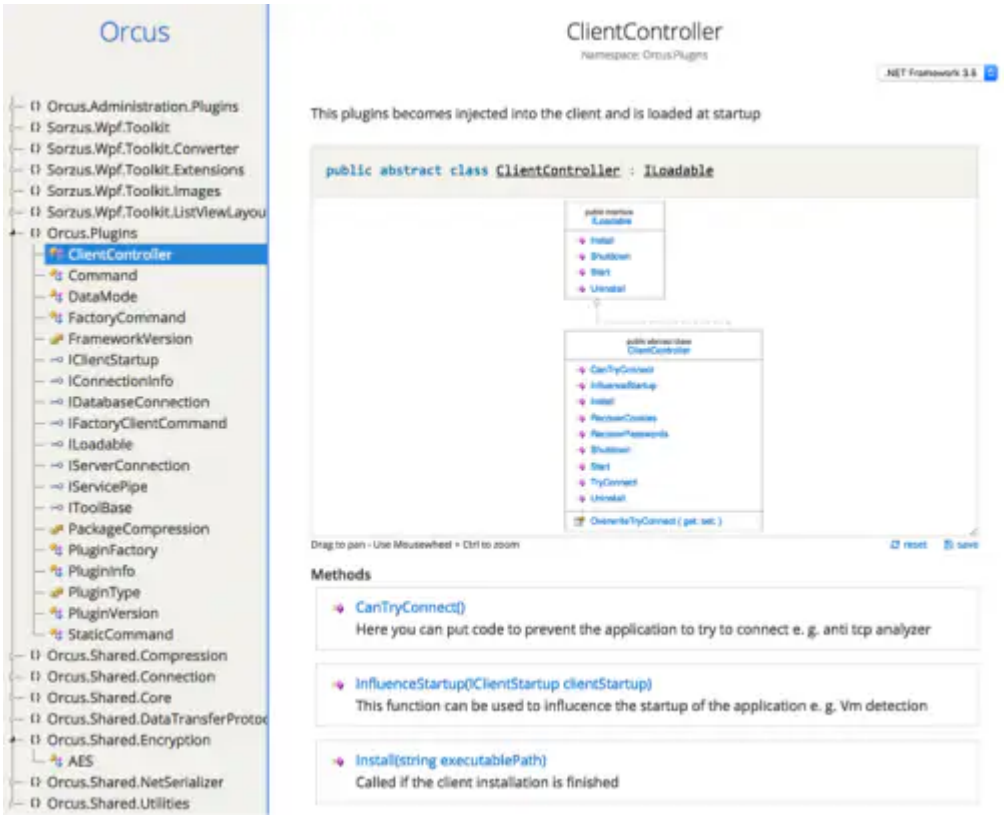

Figure 6 Example of a plugin library documentation

The Real Time scripting feature allows Orcus users to write and execute code (C#, VB.Net) in real time while remotely managing the compromised system.

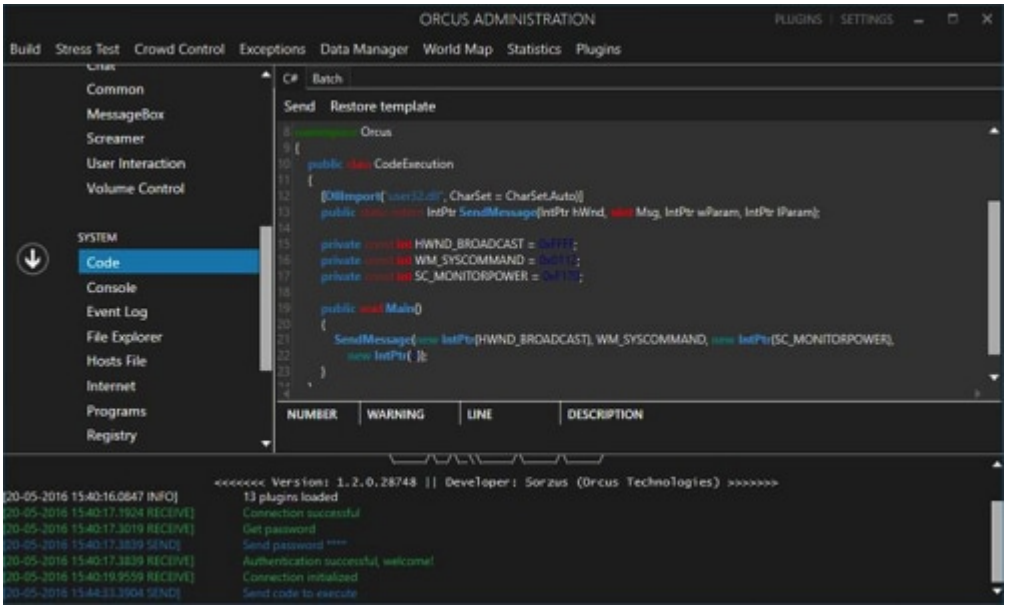

Figure 7 Real time scripting feature on Orcus

Analysis: Orcus Protections

From an incident responder or threat analyst's perspective, it is important to understand the type of anti-analysis protections a malware family employs so one is able to build an environment to successfully analyze the malware. This blog is not intended to discuss reverse-engineering the RAT in detail; however, it is interesting to see some of the anti-analysis features which Orcus employs to avoid being detected in a standard analysis environment.

We reverse-engineered one of the Orcus samples seen on a recent attack to check and verify some of the configured features. Given Orcus is developed in C# / VB.Net, we can easily peek into the code using a .NET disassembler. If an Orcus user enables the VMDetection feature while building the malware binary, the malware would check if the malware is running within a virtual machine environment. The virtual machines that Orcus detects are ParallelsDesktop, VirtualBox, VirtualPC and VMWare. The figure below shows the code excerpt for detecting the presence of virtual machines.

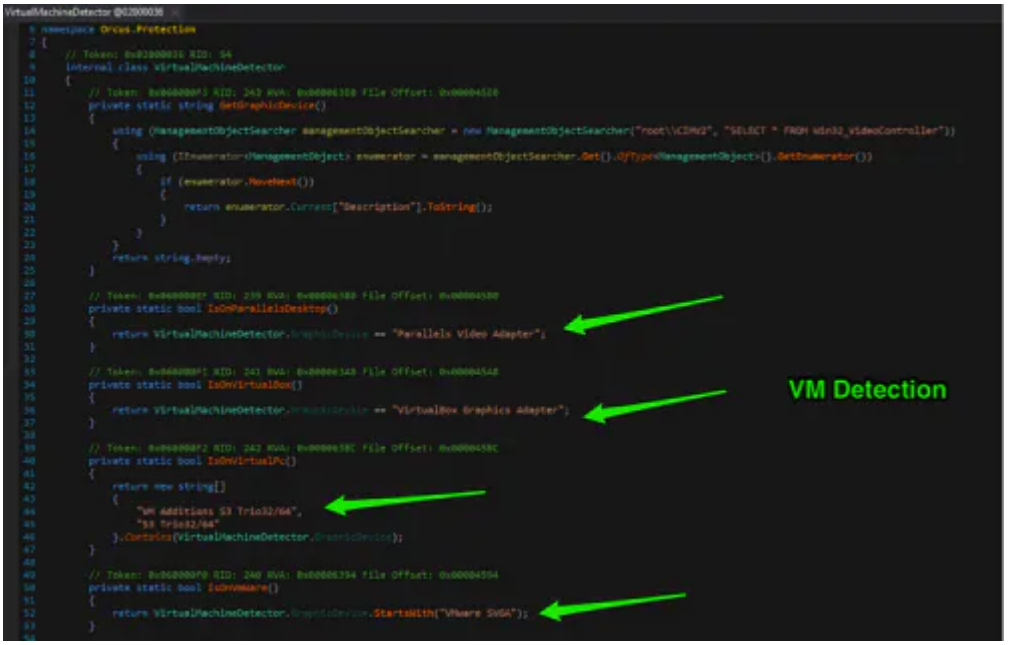

Figure 8 Virtual Machine detection in Orcus

Orcus also checks for processes of network monitoring tools like Netmon, TCPView and Wireshark as shown in the figure below.

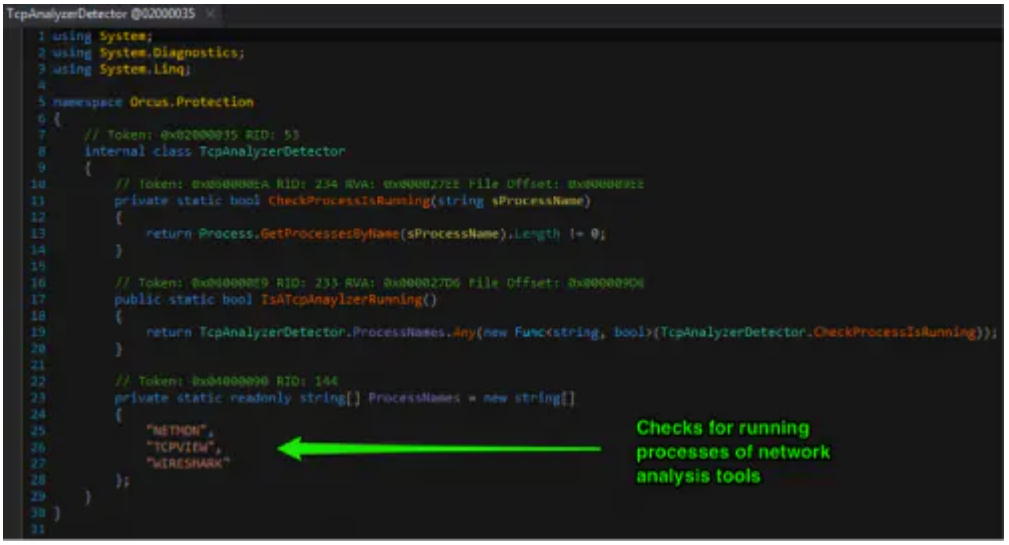

Figure 9 Detection for network analysis tools

Impact

Figure 10 below shows the trending graph seen in Autofocus on the number of malware download sessions for Orcus. Given the feature rich toolset and the scalability Orcus provides, it is not a surprise that the usage and acceptance of the Orcus RAT is growing among cyber criminals since being first sold early this year. Given the increasing popularity of Orcus, it is likely that we will see more cyber crime campaigns where the RAT of choice is Orcus.

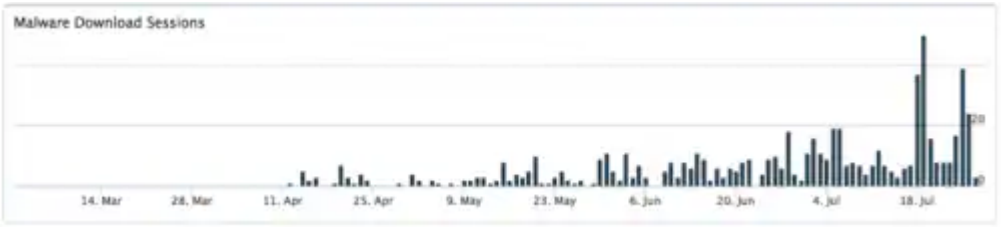

Figure 10 Autofocus graph of Orcus download sessions over time

Conclusion

The individuals behind Orcus are selling the RAT by advertising it as a "Remote Administration Tool" under a supposedly registered business and claiming that this tool is only designed for legitimate business use. However, looking at the feature capabilities, architecture of the tool, and the publishing and selling of the tool in hacker forums, it is clear that Orcus is a malicious tool, and that its target customer is cyber criminals. It's not uncommon but this is an interesting case where a developer with an initial intention to release the code for free or open source, ends up in collaborating with an individual in a hacker forum who has prior experience in building and selling similar malicious tools, and creates a commercial RAT which has started to gain wide acceptance among cyber criminals with its unique feature set and flexible architecture.

Palo Alto Networks WildFire correctly identifies Orcus as malicious and AutoFocus customers can track this threat using the Orcus tag.

IOCs:

The current list of hashes for Orcus samples can be found on the Unit 42 github page here.

Source: https://unit42.paloaltonetworks.com/unit42-orcus-birth-of-an-unusual-plugin-builder-rat/